The Cybersecurity Game Master

From Role Playing Games to Tabletop Exercises that Engage and Inspire

Roberto Dillon

CRC Press
Taylor & Francis Group

The Cybersecurity Game Master

From Role Playing Games to Tabletop Exercises that Engage and Inspire

Roberto Dillon

CRC Press
Taylor & Francis Group

The Cybersecurity Game Master

In today's digital landscape, no company is immune to cyberattacks, making preparedness essential for any organization, regardless of size. Enter the world of Tabletop Exercises (TTXs), a cost-effective and results-driven approach to test cyber crises proactively. However, workplace dynamics can hinder effective participation as the fear of proposing wrong decisions and the apprehension of appearing less competent in front of colleagues can still stifle creativity, even during a simple exercise. This book addresses these concerns by injecting a fresh perspective, seamlessly integrating elements from Role-Playing Games (RPGs) into the design and execution of TTX scenarios to make them more engaging and fun. *The Cybersecurity Game Master* invites readers not only to master the TTX mindset but also to embrace it as a gamified experience, fostering a dynamic learning environment without the fear of judgment. By infusing fun into the serious business of cybersecurity, this book redefines TTX design, allowing teams to enjoy the process of understanding their company, procedures, and future challenges in a stress-free manner.

Associate Professor **Roberto Dillon** holds a Ph.D. in Computer Engineering from the University of Genoa, a postgraduate Certificate in Cybersecurity from the Rochester Institute of Technology, and a Higher Education Teaching Certificate from Harvard. Over the years, he has published several books with CRC Press, AK Peters, and Springer, sharing his insights across game design and cybersecurity, two fields that have shaped his life since childhood. His journey began in the mid-1980s, programming games on a Commodore 64 and, later, on a beloved Commodore Amiga, which was once infected by an early virus lurking on a floppy disk. That experience sparked a lifelong curiosity about how systems

work and how they break. Today, he is an IEEE Senior Member and an (ISC)² Professional Member, with a career that bridges creative innovation and design with the practical realities of digital security.

The Cybersecurity Game Master

From Role Playing Games to Tabletop Exercises that Engage and Inspire

Roberto Dillon

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

Designed cover image: Shutterstock ID: 1230552220

First edition published 2026
by CRC Press
2385 NW Executive Center Drive, Suite 320, Boca Raton FL 33431

and by CRC Press
4 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN

CRC Press is an imprint of Taylor & Francis Group, LLC

without intent to infringe.

ISBN: 978-1-032-99820-6 (hbk)
ISBN: 978-1-032-99851-0 (pbk)
ISBN: 978-1-003-60631-4 (ebk)

DOI: 10.1201/9781003606314

Typeset in Caslon
by Apex CoVantage, LLC

Dedicated to the Memory of Prof. Agostino Bruzzone
(1965–2025)

Contents

About the Author

Associate Professor **Roberto Dillon** is an (ISC)² Professional Member, an IEEE Senior Member, and the author of six books published by A.K. Peters, CRC Press, and Springer. He holds a master's degree and a Ph.D. degree in computer engineering from the University of Genoa, a MicroMasters Certificate in Cybersecurity from the Rochester Institute of Technology, and a Certificate in Higher Education Teaching from Harvard University.

Currently, he serves as the Academic Head for the School of Science and Technology at James Cook University's Singapore Campus, where he established a dedicated Cybersecurity degree program in 2020 and founded Southeast Asia's first permanent Computer Games Museum in 2013. Before joining JCU, he held academic positions in institutions such as The Royal Institute of Technology (KTH), Nanyang Technological University, and the DigiPen Institute of Technology.

A keen supporter and developer of Free Open-Source Software (FOSS), his research interests focus on serious games design and on different areas of cybersecurity such as User and Entity Behavior Analytics (UEBA), Open-Source Intelligence (OSINT), and threat intelligence. As a professor and educator, he is also very passionate about enhancing capacity building for the next generation of cybersecurity experts in Southeast Asia by designing new curricula and innovative gamified training tools. Feel free to reach out via his homepage: https://robertodillon.nicepage.io

Foreword

Pause for a moment and think about the world we live in today. Technology is advancing at breakneck speed, reshaping industries, and redefining our daily lives. But amid all this innovation, one truth remains unchanged: no matter how advanced your tools are, the true strength of any cybersecurity program lies in its people. The human element – their creativity, resilience, and quick thinking under pressure – is the frontline defense against ever-evolving threats.

This book is built on that understanding. It's a reminder that resilience isn't just about technology, processes, or compliance checklists. It's about nurturing teams who can adapt, improvise, and collaborate when the unexpected strikes. These teams don't simply follow a script – they write their own story in real time, balancing logic with instinct and protocols with creativity.

So how do we build such teams? This is where tabletop exercises (TTXs) come alive. When designed thoughtfully, they are more than drills – they are rehearsals for reality. They allow teams to test their judgment, challenge their assumptions, and practice responding to chaos in a safe, controlled environment. And when storytelling is woven into these exercises, something magical happens. The room stops feeling like a meeting and starts feeling like a mission. People lean in, take ownership of their roles, and bring their full selves to the table.

What this book offers is a fresh way to think about cybersecurity readiness. It invites us to borrow from the world of role-playing games (RPGs), where players face challenges, adapt to twists, and grow stronger through experience. The facilitator becomes a game master, guiding the

team through realistic scenarios where technical skills and human imagination meet.

But make no mistake – this approach doesn't replace operational rigor. It enhances it. By blending narrative with structure, you create learning experiences that are engaging, repeatable, and impactful. You build not just knowledge, but muscle memory. And in the heat of a real incident, that muscle memory can make all the difference.

In these pages, you'll find a thoughtful framework for making resilience a living, breathing part of your security culture. Whether you're a seasoned leader, an aspiring analyst, or a curious learner, my hope is that this book inspires you to see incident response not as a checklist, but as a craft – one where the human spirit is just as important as the latest patch.

So gather your team. Roll the dice. And prepare not just to defend your organization, but to lead it through the challenges ahead.

Enjoy the journey.

Dr. Magda Chelly,
Co-Funder and CEO
RiskImmune (By Responsible Cyber)

Preface

Role-Playing Games (RPGs) and training exercises. Fantasy and Cybersecurity. At first sight, these look like completely different domains that have nothing in common. And yet, when we look a little closer, we begin to see the potential of this strange alliance, an alliance that holds the key to transforming how we prepare for the inevitability of cyber crises in a world of escalating digital complexity.

In this book, I want to explore how we might bridge the serious business of cyber defense with the imaginative power of storytelling and structured gameplay. Whether we like it or not, the threat landscape keeps changing radically and, with it, our approach to training, preparedness, and organizational resilience must evolve too.

We are no longer dealing with a world of isolated breaches or opportunistic hackers looking for a quick win. We are now contending with persistent adversaries, professionally coordinated attack groups, and nation-state actors whose campaigns unfold over weeks, months, and even years. Ransomware has become a commoditized service. Supply chains are compromised through subtle, deeply embedded tactics. Phishing is no longer just a mass spam. It is now a hyper-targeted, socially engineered spear-phishing backed by months of reconnaissance. And yet, for many organizations, cybersecurity training remains stuck in another era: annual compliance modules, uninspired webinars, check-the-box simulations, and static TTXs. These formats may fulfill an obligation, but they rarely cultivate instinct, teamwork, or adaptability. In short, they are not preparing us for the dynamic chaos of a real incident. Worse still, they are boring.

Ask yourself: how much do your teams retain from their last training? Can they recall the communication flow during a crisis? Do they know who owns what role under the Incident Response Plan (IRP)? Can they detect when an event transitions from inconvenience to emergency? These are not questions of policy; these are questions of people and how they engage with complexity under stress and time pressure. That's where gamification comes in.

Mind you, I always hated buzzwords and how they are used to make simple concepts more mysterious and, way too often, the domain of self-proclaimed experts. Unfortunately, "gamification" was no exception but, as you will see, here we will not treat it as a gimmick but as a necessary cornerstone for the evolution of training practices.

At their core, RPGs are not about elves and dragons. They are about collaborative storytelling, decision-making under uncertainty, and reacting to consequences. They provide a structured environment where participants can take on specific roles, make choices, and see how those choices ripple out into the world. If that sounds familiar, it's because it mirrors the very essence of cybersecurity incident response. The difference is that RPGs do it in a way that pulls you in, rather than pushing you through.

So, what if we take the proven principles of RPG design and apply them to our cybersecurity exercises? What if instead of walking through a checklist, our response teams were characters in a high-stakes scenario, with clear roles, evolving threats, unexpected twists, and the need to collaborate, adapt, and overcome? What if, instead of a mere facilitator, we have a "Cybersecurity Game Master" instead, orchestrating an evolving scenario filled with narrative tension and realistic consequence?

This book was born from that question. It is the result of years of game design experience building immersive experiences coupled with scenario-based teaching and trainings. From now on, participants should not be simply told what to do, but they should figure it out, together, in a simulated crisis that feels just real enough to matter.

The structure of the book reflects this philosophy. You will find scenario playbooks that follow familiar incident response frameworks, referencing

MITRE ATT&CK® techniques and real-world threat vectors, from distributed denial-of-service (DDoS) and ransomware to phishing. Proposed exercises include injects, alternative outcomes, and skill checks designed to simulate real pressures and unexpected outcomes. Just like in a real breach, your decisions have consequences. And failures can happen, too.

More importantly, though, this approach injects life into what can otherwise feel like a chore and aims at turning passive learners into active participants, it encourages teams to speak, argue, plan, and reflect. It reveals communication breakdowns, role confusion, or procedural gaps before a real attack tests them. And it does all this without needing a multimillion-dollar cyber range: just some time, commitment, and a willingness to treat training as a story worth telling.

Of course, this book is not just about rules, rolling dice, and scripts. Its real objective is to foster a proper company culture that focuses on readiness and shared responsibility in cybersecurity. And this can only arise from honest and committed teamwork. It cannot be created through fear or obligation: it grows through engagement, through relevance, and yes, even through “excitement” and “fun”.

I’ve worked with teams of students and professionals alike across different sectors and the message is always the same: training only works when it feels real, and, even more importantly, when people care. That doesn’t mean turning every exercise into a show, but it means creating space for emotion, pressure, and choice and that’s exactly what the RPG format gives us, including the ability to care for our alter ego in the virtual world.

To be clear, there are no such things as silver bullets. The proposed approach to gamified training still needs to be grounded in good documentation, specific tools, legal counsel, and executive buy-in. Once the frameworks are in place, though, what remains is the people making up the team and how well those people come together, under stress, and make decisions that protect the organization to mitigate and recover from the consequences of an attack.

That’s the heart of this book. That’s the reason for blending the serious world of cybersecurity with the playful structure of role-playing: if we want our people to thrive during the next inevitable incident, and not just (hopefully) survive it, we must train them in ways that reflect the complexity of both the threat and the team internal dynamics.

Whether you are a CISO, an instructor, a security analyst, a policy maker, or just someone who believes training can be better, I invite you to explore the chapters ahead with an open mind. Read the scenarios, adapt them to your environment, and above all, play them. The stakes are high, but so too is our ability to prepare.

Let the adventure begin. Are you ready?

Roberto Dillon

Genoa, 15/6/2025

Acknowledgments

This book was only possible thanks to the help of several people.

First and foremost, Ms. Gabriella Williams from CRC Press, who believed in a book proposal mixing role-playing games (RPGs) and cybersecurity training, surely not something you hear every day, and decided to trust me in this original endeavor.

I am also highly indebted to Dr. Magda Chelly for her Foreword, to Ms. Francesca Bosco for taking the time to answer all my questions for the interview section, providing valuable insights from different perspectives, to Dr. Arushi, for proof-reading the early draft, as well as to the all the Strategos master's degree students, in particular, Mr. Seyed Mahdi Seyedishandiz and Mr. Alireza Asgari, for playtesting the scenarios with me.

Prof. Agostino Bruzzone passed away while the book was in production. He was a great professor, a dear friend, and a truly inspiring scientist and engineer. He will be sorely missed, and this book is dedicated to his memory.

PART 1

FROM FACILITATOR TO CYBERSECURITY GAME MASTER

1

The Purpose of Tabletop Exercises

DOI: 10.1201/9781003606314-2

Welcome to an increasingly technologically driven world, where innovative ideas, services, and products keep making both our personal and professional lives easier and smarter! It all sounds wonderful and, for the most part, it is, but, unfortunately, there is always another side of the coin. Transferring everything online for every company in every field, in fact, has brought over a new and very significant risk in the form of a relentless barrage of cyberattacks including data breaches, ransomware, denial of service, identity theft, espionage, and more [1]. New teams have to be formed to address these challenges and new programs for training and awareness have to be devised so that the right people are ready to address any upcoming challenge with a cool head, without panicking, even when under tremendous pressure from colleagues, clients, stakeholders, and everybody else around them. Such almost ascetic calm and effective attitude can only be achieved by proper training and once confident in the resources and procedures available. Simulating possible crises many times to review not only the possible incidents that may occur but, most importantly, the procedures that need to be executed to counter them is a must, and, among all the tools and strategies that are used nowadays, one of the most interesting – without a doubt – is the so-called “Tabletop Exercise”, or TTX.

TTX, in fact, provides a unique and straightforward way to test and brainstorm any possible scenario by bringing the relevant people together and make them analyze the problem in detail, in a step-by-step manner. Moreover, generally speaking, TTX don't even require any additional equipment to be setup or any further investment to be deployed successfully; hence, they should be easily embraced by upper management as their benefits to any team can hardly be questioned and there is no valid excuse to reject them.

What Is a Tabletop Exercise (TTX)?

Sounds almost too good to be true, so what is a TTX exactly and how can it help us in practice? TTXs are simulated scenarios designed to assess an organization's readiness and response capabilities in the face of a specific cybersecurity incident. Unlike real-world incidents, though, TTX unfolds just on paper, allowing participants to brainstorm and collaboratively navigate through the hypothetical steps of an ongoing incident without real-world consequences. Think of it as a strategic cybersecurity rehearsal, where the goal is not limited to identify vulnerabilities but, most importantly, to check, verify, brainstorm, and refine response strategies to enhance the company's overall resilience and cybersecurity posture.

Essentially, a TTX then plays out like a sort of "Theatre of the Mind", a concept that was first adopted in the early days of radio broadcasting, when listeners were supposed to play out a narrative in their minds as it was described by the speaker on the radio, and then made popular in "Dungeons & Dragons" (D&D) role-playing games (RPGs) where players had to "visualize" the adventures of their alter ego in a fantasy world based on the description and narration of a game master (GM). Here too, in fact, the participants need to relate the ongoing description of the chosen incident to their specific infrastructure and act accordingly to mitigate and resolve any issues and possible breaches.

But there is neither any game nor any exercise without players or participants, so who are the participants in a TTX supposed to be?

TTX participants can essentially be divided into two groups: the team and the facilitators.

It is important to understand that the specific composition of the team needs to consider the perspective of the exercise itself for the TTX to be truly effective and meaningful. This means that, if the exercise wants to be more technical in nature, the team should include the IT and cybersecurity technical guys in addition to at least one of their managers. If the TTX aims at discussing more high-level risk management or governance issues, for example, the team should include upper management and C-level executives instead and leave the “geeks” at their desks undisturbed.

The facilitators group, on the other hand, includes a “moderator” (sometimes also referred to as the “narrator” or just as the “facilitator”), responsible not only for leading the session but also for defining the topic and scope of the TTX itself. He/she will set up the exercise, introduce the topic, the rules, and then guide the team throughout the session. Besides the moderator, this group should also include a “scribe”, whose role is like minutes-taking in a normal meeting, to keep track of the progress of the exercise and record anything of note that gets discussed. Having these materials at hand later is, indeed, crucial as the TTX should always be followed by a retrospective session where all the participants need to discuss any findings and possible inconsistencies, doubts, or unexpected situations that emerged during the exercise itself.

Do note that, as recommended by common agile project management practices, a TTX, like all other meetings, should have a predefined time-boxed duration to avoid wasting time and resources. In this case, we are talking of a typical duration between 30 minutes and two hours. The retrospective should instead be between 30 minutes and one hour only. Generally speaking, management-oriented exercises should lean towards shorter time frames while technical ones can easily require more time.

The Documents

It was mentioned in the previous section that a TTX can discuss many different security aspects for a given company, from a technical perspective, a management one, or anything in between. In any case, whether the TTX aims at being more technical or more strategic in nature, it has to reflect the specific nature and posture of the company itself. These should be clearly defined beforehand in a set of documents that will act as the guidelines the participants have to rely on and refer to during the exercise. It is expected that all the participants should already be familiar with the required guidelines and procedures illustrated in such documents, which usually take the form of an Incident Response Plan (IRP) and one or more incident playbooks. These are related elements within the broader field of cybersecurity incident management, but they serve different purposes, and, before we proceed further, we need to have a very clear idea of their basic structure and goals to use them effectively.

Let’s start by defining what the IRP is.

The Incident Response Plan (IRP)

An IRP is a comprehensive, high-level document that outlines the overarching strategy and procedures an organization follows in response to any cybersecurity incident. It serves as a guiding framework and typically covers various aspects of incident response, including roles and responsibilities, communication protocols, escalation procedures, and the overall workflow from incident detection to resolution. The IRP is often a foundational document that sets the stage for how an organization approaches incidents in general.

To recap, a well-written IRP has to provide the following:

1. Broad Scope: the IRP encompasses a wide range of potential incidents, outlining general response strategies applicable to different types of cybersecurity events.
2. Strategic Guidelines: it needs to cover high-level strategic guidance for incident response but may not go into the detailed, specific steps for

each type of incident (as detailed procedures are usually discussed in other documents such as the playbook).
3. Framework: it has to establish the overall framework to be followed for an incident response situation. This is often articulated into sub-sections dedicated to detection, containment, eradication, recovery, communication, and lessons learned.

The Incident Playbook(s)

An incident playbook, on the other hand, is a more focused and tactical document. It is a collection of specific, detailed procedures and steps to be followed for a particular type of incident. Playbooks are more granular and are designed to guide the incident response team (IRT) through the specific actions and decisions necessary to address a predefined scenario as it unfolds in real life.

Playbooks are often created based on the organization's experience, industry best practices, and lessons learned from previous incidents.

An incident playbook needs to have:

1. Specific Incident Focus: for example, covering a ransomware attack, data breach, or DDoS attack.
2. Detailed Procedures: it has to provide step-by-step instructions for the IRT to follow during the handling of a specific incident. These must be followed to the letter and need to be thoroughly tested.
3. Response Automation: where applicable, it may also include references and instructions on how to deploy and run automated responses or scripts to streamline and accelerate certain response tasks.

Table 1.1 summarizes the key points of both documents while sample templates to be customized for specific needs are provided in Appendices A and B, respectively.

In summary, while the IRP establishes the high-level strategy and framework for responding to cybersecurity incidents, telling us the "What" and "Why" of incident response, incident playbooks are specialized

documents that provide specific guidance for handling individual crises, essentially telling us “How” to resolve them. Both are essential components of a robust cybersecurity incident management program, working together to ensure a well-coordinated and effective response to security events.

Table 1.1 The key elements of an IRP and a playbook ⏎

ASPECT	INCIDENT RESPONSE PLAN (IRP)	PLAYBOOK
Scope	Broad, covering all types of incidents	Narrow, focused on specific incident types
Level of Detail	High-level framework	Detailed, step-by-step instructions
Purpose	Strategic: Defines roles, processes, and goals	Tactical: Provides actionable guidance
Example for Ransomware	Outlines who responds, communication protocols, etc.	Specifies how to isolate systems, restore data, etc.

Most importantly for us, these documents must also be at the heart of a well-planned exercise, not only because a TTX may be designed with the specific purpose of testing a particular playbook, for example, but also as a reference tool that each participant should have readily access to for consultation as the incident unfolds and new probing questions and problems emerge.

With this set of documents ready, every manager then has a simple, straightforward, but fundamental question: can this supporting documentation, upon which the whole security of our business is built upon, actually pave the way out of the woods or will it fail for whatever reason when we most need it? Well, that is exactly what a well-designed TTX should help us to find out!

No Documents? No Problem!

If TTX are made to test all the existing strategies and solutions outlined in the documentation, does this mean that TTX can only take place in companies that already have such a mature set of strategies laid down? Not necessarily. TTX are in fact a very flexible tool and they can also be used in the process of creating such documents, by helping us reflecting and focusing on new incidents that can otherwise take our business by surprise.

In this case, though, a fundamentally different approach is needed where the TTX itself sets up the scene for brainstorming such documents instead of being built from the ground up to test them. For this purpose, I would recommend running the exercise around existing serious games designed with the specific intention to have the team's "creative juices" flow and reflect upon every action they take and threat they face.

A great tool that matches our goal is the well-known card game "Backdoors & Breaches" designed by Black Hills Information Security and Active Countermeasures [2]. The core version of Backdoors & Breaches contains 52 cards to simulate many different types of attacks articulated into the various phases of the cybersecurity kill chain [3], that is, the different steps that organized hacker groups follow in real life attacks.

While playing the physical version of the game is likely going to be a more satisfying experience; the game can also be run online [4]. Here, a moderator starts by drawing a random card for each main phase of the simulated attack (i.e., Initial Compromise, Pivot & Escalate, Persistence, C2, and Exfiltration), hence defining the scenario to be practiced. On the other hand, the team has access to a set of "Procedure" cards that provide the kind of information that should be outlined in the actual playbooks. As the moderator builds a narrative matching the available cards in hand, the team has to follow up by discussing the most appropriate procedures to fight the ongoing threat. Once they pick a relevant card, its effect is determined by a D20 (i.e., a 20-sided die) roll. If the procedure selected is both successful and appropriate for the situation (as judged by the moderator), the corresponding attack card is uncovered and removed. If not,

the team receives appropriate feedback from the Narrator and then must try something else, selecting another card and starting another round. If, after ten rounds, the unique challenges exemplified by the different attacking cards have been properly addressed, the team wins.

A simpler alternative game that I designed to introduce my cybersecurity students to different concepts and to illustrate how basic attacks unfold is “PeriHack” [5]. The game is designed to be highly customizable and expandable to suit different environments and situations, but, in its basic form downloadable from [6], it provides a sample board representing a generic network and company premises (Figure 1.1).

The game is played by two players or teams, each taking either the red-team (attacker) or blue-team (defender) role. By playing the game, as summarized in [7],

> the former can gain a better understanding of how a cyber-attack can start and evolve, while the latter can appreciate the struggle of managing a multitude of possible weaknesses with limited resources, thus the need to make decisions based on perceived priorities and limited information. The game requires players to investigate a sample network for vulnerabilities and chain assaults to exploit technical and social engineering exploits. In addition, it replicates budget limits for the blue team by providing restricted resources to examine and prioritize significant risks.

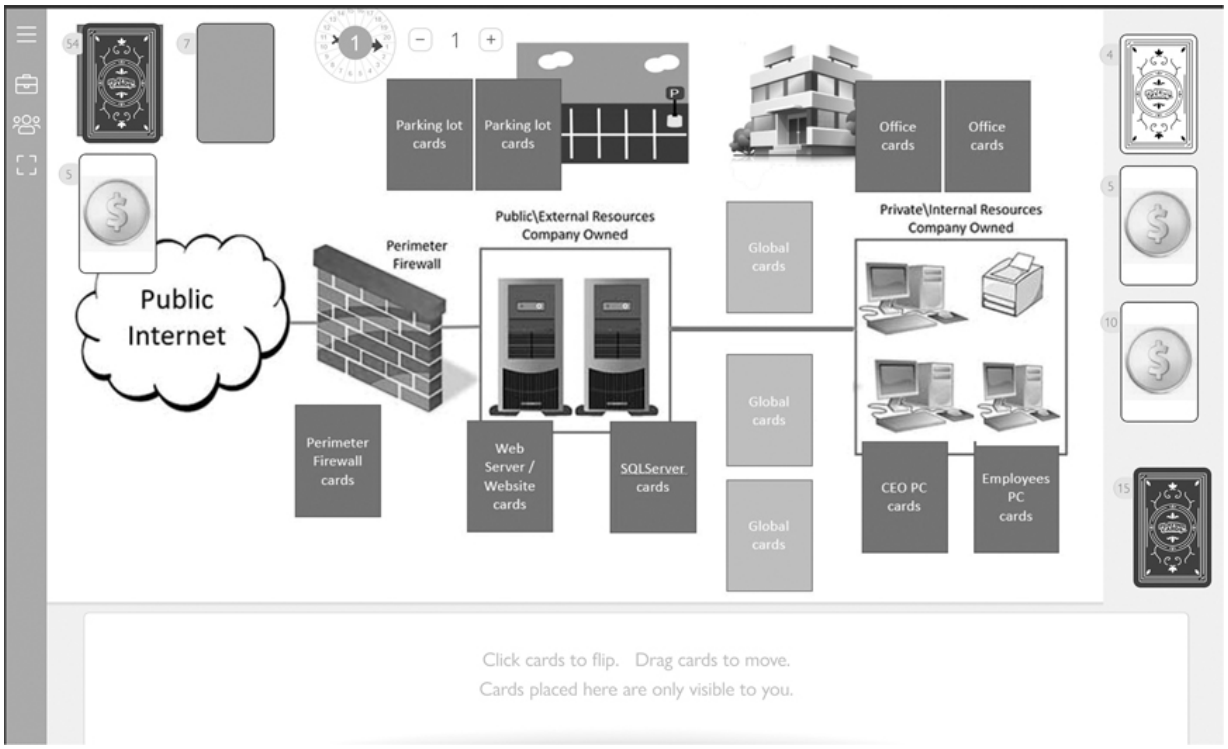

Figure 1.1 The PeriHack board. All the game materials and rulebook can be downloaded from its GitHub repository [6]. ⏎

In our specific case, the moderator can also design a new layout to give a better representation of the specific company infrastructure if needed, and then take the role of the attacker, while the other participants focus on the defensive side of things and brainstorm the best strategies. Like in “Backdoors & Breaches”, both the red and blue teams here are also dealt different cards, outlining possible attacks and mitigation strategies that are then played against each other by using both a D20 roll plus any eventual modifiers to check whether a specific action is successful or not.

By playing these games and see a random attack unfolding, the team has a unique opportunity to reflect on the proper actions that must be taken to mitigate the consequences and ultimately resolve the incident within their specific context. This allows for a proper assessment of the company’s security posture and of the most suitable procedures that can then be written down to define the core points of the playbooks and IRP.

References

1. R. Dillon, P. Lothian, S. Grewal and D. Pereira. “Cyber Security: Evolving Threats in an Ever Changing World”, in *Digital Transformation in a Post-Covid World: Sustainable Innovation Disruption and Change*, CRC Press, pp. 129–154, 2021. ⏎
2. https://www.blackhillsinfosec.com/projects/backdoorsandbreaches/ ⏎
3. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html ⏎
4. https://play.backdoorsandbreaches.com/ ⏎
5. R. Dillon and Arushi. “‘PeriHack’: Designing a Serious Game for Cybersecurity Awareness”, in *IEEE International Conference on Teaching, Assessment and Learning for Engineering (TALE)*, IEEE, 2022. ⏎
6. https://github.com/rdillon73/PeriHack ⏎
7. Z. Batzos, T. Saoulidis, D. Margounakis, et al. “Gamification and Serious Games for Cybersecurity Awareness and First Responders Training: An Overview”. *TechRxiv*. https://doi.org/10.36227/techrxiv.22650952.v1, 2023. ⏎

2
Planning and Running a TTX

DOI: 10.1201/9781003606314-3

TTXs are all about planning, testing, and training incident response procedures. To start planning one, we need to have a thorough understanding of incident response frameworks and related best practices first, regardless of whether the company's documentation is already available or not. To help us in this regard, there are different frameworks that we may adopt, including the NIST 800–61 and MITRE ATT&CK, whose best practices can be readily applied in the context of a TTX.

Using NIST 800–61 to Drive TTX Design

Among the different frameworks that crystallize cybersecurity knowledge and proven best practices, the National Institute of Standards in Technology (NIST) 800–61 is one of the most well-known and widely adopted [1].

There, the incident response process is described as a looping sequence consisting of four main phases (Figure 2.1):

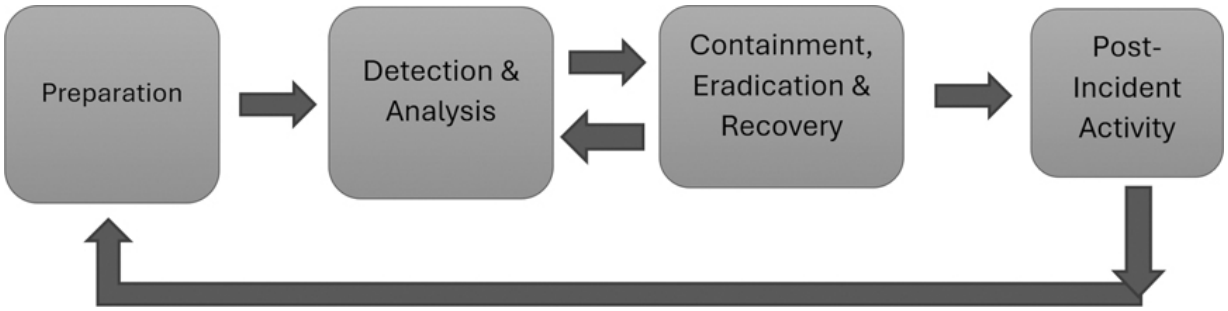

Figure 2.1 Incident response life cycle as outlined in NIST 800–61. ⏎

Preparation (Phase I) is all about setting up the stage to be ready for whatever challenge may arise. Preparing the relevant plans and playbooks we introduced earlier, as well as organizing regular TTX with the relevant team members, is at the core of this phase. The NIST guidelines put a strong emphasis in establishing clear communication channels at all levels as well as having dedicated and stand-alone workstations and/or laptops to analyze data, perform forensic analysis, etc. Updated information on critical assets, such as database servers, as well as hashes of critical files to verify their integrity should be readily available to be referenced whenever needed, too.

Detection and Analysis (Phase II) is concerned with identifying possible attack vectors and is an important source of inspiration for planning the beginning scenario of a TTX.

The most common attack vectors include the following:

- **External/Removable Media**, for example, a bad USB drive.
- **Attrition**, for example, DDoS or brute force attacks targeting an authentication system.
- **Web**, for example, XSS, SQLi, etc.
- **Email**, for example, phishing and sending malicious file attachments.
- **Impersonation**, for example, spoofing, man-in-the-middle, rogue access point, etc.
- **Improper Usage**, for example, breaches of established acceptable usage policies due to honest mistakes or insider threats.

- **Loss or Theft of Equipment**, for example, the CEO goes to an event and loses his authentication token or loses his smartphone.

Ideally, a company should have relevant playbooks to address each of these possible incidents. In any case, regardless of the possible attack vector, determining whether an incident has actually occurred (false positives are always a common occurrence) and then assessing its magnitude is the first and most critical task. For this, we need to analyze a set of indicators (often simply referred to as “IoC”, i.e., “Indicators of Compromise”). Common indicators are alerts from antivirus software, log entries, reports from IDS, IPS (Intrusion Detection, or Prevention, Systems), or SIEM (Security Information and Event Management Systems), and so on.

Once an incident has been confirmed and identified, its severity can be assessed in multiple ways, for example, by profiling and comparing the normal and expected behavior of each system with the actual performance. Now we see the importance of the previous “Preparation” phase, which helps us in establishing an original “snapshot” of the resources that can be negatively impacted and provides us with a baseline we can use to compare any changes in configuration and performance. In this second phase, we also need to prioritize incidents (we can’t always be so lucky to have a single incident at a time, can’t we?) according to their impact and have a solid documentation procedure, including a chain of custody, if applicable. Last but not the least, we need to establish clear directives on who should be notified and involved in the next phases of the process (e.g., the Chief Information Security Officer (CISO), the system owner, PR and/or legal departments).

Next comes the **Phase III** and what many people would consider as the most critical part of all: **“Containment, Eradication, and Recovery”**. This phase may also imply some back and forth with “Detection and Analysis” to verify that our ongoing actions have the expected results. Containment is indeed critical to prevent current infections from spreading further and requires ad-hoc and often drastic actions, like shutting down a system or disconnect it from the network. These need to be outlined in advance via

corresponding playbooks tailored for different relevant incidents, possibly including malware infections spreading via email, network-based DDoS attacks, and so on.

Across these phases it is also very important to collect any relevant evidence, as this will be needed not only for possible attribution and legal suits to follow but also to strengthen the overall posture and strategies during the last part of the process, **Phase IV**, a.k.a. **"Post-Incident Activity"**, where the team has to focus on all the relevant lessons learned from the incident. Relevant questions to answer may include the following:

- Incident Questions (IQs)
    - What happened exactly and at what time?
    - How did the incident progress?
- Action Questions (AQs):
    - How well did the staff perform under pressure?
    - Were all the required procedures followed?
    - Were they good enough or was there anything missing? If so, what can be improved?
    - Anything that could have been done differently?
- Process Questions (PQs):
    - Was information sharing within the organization and with relevant outside entities (e.g., for regulatory requirements) effective and smooth?
- Strengthening Questions (SQs):
    - Can we adopt additional corrective actions and tools to improve our posture and prevent similar incidents from now on?
    - Is there any new or more reliable IOC that can point out a similar incident even earlier?

From this brief introduction, we can see how the NIST framework can also be an invaluable tool to guide us in the process of a simulated situation at the center of a traditionally planned TTX and help to plan the preliminary steps of a suitable case study.

TTX Example I

Let's imagine we want to plan an exercise to test what could happen if the laptop of a C-level executive gets stolen during a conference, that is, "Loss or theft of equipment", as categorized in the Detection phase of the NIST framework.

How shall we introduce the topic and set the exercise up accordingly?

First, the team. This kind of situation is interesting as it should involve a variety of people with different profiles in the organization, including the victim of the theft, the IT personnel, and, potentially, also someone from the legal and PR departments as well.

The Facilitator could introduce the exercise by announcing the following scenario:

> *In the bustling halls of a technology conference, where innovation electrifies the air and networking is a common goal, an unfortunate incident unfolds. Our CEO is diligently attending seminars and engaging in industry discourse. After a coffee break, he is back for the next meeting with a possible partner only to find their laptop missing from their bag! The device contained a treasure trove of sensitive information, including product details of our next launches and crucial account credentials, and it may have now fallen into the wrong hands.*

To make the scenario even more relevant and sell the exercise to the executives in the room, it is also a good practice to outline the potential impact, financial or otherwise, that the incident may have, as recommended by $(ISC)^2$ in [2]. For this, any of the following points could be emphasized according to the nature of the business being portrayed:

1. **Data Breach Fallout:** The compromised laptop harbors sensitive company secrets, including product roadmaps, upcoming events, and strategic plans. A breach could expose these confidential details, handing competitors a significant advantage and tarnishing our market position and reputation.
2. **Financial Ramifications:** With account information and passwords stored on the stolen device, the company faces the grim prospect of unauthorized access to its financial accounts. Malicious actors could exploit this access to siphon funds, execute fraudulent transactions, or manipulate financial records, potentially resulting in substantial monetary losses.
3. **Reputational Damage (RD):** Trust is critical in business, and a data breach stemming from the theft of the CEO's laptop can shatter the company's reputation. If not properly managed, news of the incident spreading among clients, partners, and stakeholders could erode trust and confidence in the company's ability to safeguard sensitive information, leading to loss of clientele and business opportunities.
4. **Regulatory Penalties:** Depending on the jurisdiction and industry regulations applicable to the company, the fallout from a data breach may extend to regulatory penalties and legal ramifications. Failure to adequately protect customer data and sensitive information can attract hefty fines and legal liabilities, further exacerbating the financial toll on the company.

Overall, the **financial loss estimates** stemming from the theft of the CEO's laptop, when factoring in potential data breach expenses, financial fraud losses, RD mitigation costs, and regulatory penalties, could easily escalate into the tens or even hundreds of thousands of dollars. However, it is important to understand the true cost of a cyberattack extends beyond mere monetary figures, likely encompassing several intangible losses such as trust, credibility, and brand value, which are often harder to quantify but equally significant in the long run.

Finally, to complete the exercise setup, the Facilitator should also be sure that a copy of the relevant playbook is available for each participant. Here, let's assume our fictitious business has established the following simple playbook for such incidents:

Cybersecurity Incident Response Playbook: Stolen Devices (e.g., laptops)

1. **Immediate Response:**

    - **Containment:** Secure the area where the theft occurred if possible. Alert relevant security to assist in identifying potential witnesses or retrieve security footage.
    - **Report Incident:** Notify relevant internal stakeholders, including IT security personnel, legal department, and executive leadership, about the theft.

2. **Assessment and Damage Control:**

    - **Inventory Data:** Determine the extent of sensitive information stored on the stolen laptop, including product details, account credentials, and any other proprietary data.
    - **Risk Analysis:** Assess the potential impact of the theft on business operations, financial security, and reputation.
    - **Communication Plan:** Develop a strategy for communicating the incident to employees, customers, partners, and regulatory authorities, ensuring transparency and accountability.

3. **Data Protection Measures:**

    - **Remote Data Wipe:** If feasible, remotely wipe the data stored on the stolen laptop to prevent unauthorized access.
    - **Password Resets:** Immediately reset passwords for accounts and systems accessed from the stolen device to mitigate the risk of

unauthorized access.
- **Encryption:** Review encryption protocols for sensitive data storage and transmission to enhance security measures.

4. **Incident Response Plan Activation:**

- **Activate IRT:** Assemble a cross-functional team comprising IT security experts, legal counsel, communication specialists, and executive leadership to coordinate response efforts.
- **Document Incident Details:** Maintain thorough documentation of the incident timeline, actions taken, and communications exchanged throughout the response process.

5. **External Engagement:**

- **Law Enforcement:** Report the theft to local law enforcement authorities and provide any relevant information or evidence to aid in the investigation.
- **Regulatory Notifications:** Determine if the incident triggers regulatory notification requirements and promptly notify applicable regulatory bodies in compliance with data protection laws.

6. **Mitigation and Recovery:**

- **Forensic Analysis:** Conduct forensic analysis of the stolen laptop, if recovered, to gather evidence and identify potential perpetrators.
- **Recovery Plan:** Implement a recovery plan to restore affected systems, strengthen cybersecurity defenses, and mitigate future risks of similar incidents.
- **Employee Training:** Provide cybersecurity awareness training to employees to reinforce best practices for safeguarding company assets, including physical ones, and preventing future security incidents.

7. **Continuous Improvement:**

- **Post-Incident Review:** Conduct a comprehensive review of the incident response process to identify areas for improvement and refine cybersecurity protocols.
- **Security Enhancements:** Invest in additional security measures, such as endpoint protection, data loss prevention, and employee awareness programs, to bolster defenses against future threats.

Notice how this simple playbook follows the different phases of the NIST framework, with an emphasis on the containment, recovery, and post-incident activities aspects.

With the scenario now well-defined and the team ready to start, the TTX could possibly unfold in a way similar to this:

Facilitator: “Our CEO, JJ, has just realized his laptop was missing from his bag and likely stolen. JJ, what are you going to do?”

CEO: “Ok, let me think … no need to panic. We got this. We have our playbook and we just have to follow the procedure … speaking of which, where is it? Oh, yes! Here it is … So, we are in the ‘Containment’ phase, right? I go to the conference security and explain what just happened.”

Facilitator: “Good. The security officer right away reports to the manager in charge and takes note of your data and the likely place where the theft may have happened. They will check any relevant security footage and keep you updated. You fill the relevant paperwork. Now what?”

CEO: “Well, I guess the fun is over and I have to reschedule all the upcoming meetings at the event to take care of this. Following the ‘report incident’ procedure, I notify our point of contacts here for such incidents. That includes. Bob (CISO), Mary (Legal) and Jean (PR). I do this from my handphone by calling them and also sending a quick email to notify the other relevant stakeholders of what happened.”

Facilitator: “Excellent. Team, the ball is on your side now.”

CISO: “Right. Now we need to assess the situation and do damage control. When did the theft happen exactly?”

Facilitator: “The conference ran on a Thursday and Friday. The theft occurred on Friday morning.”

CISO: “Ok. Since JJ’s laptop was configured to have weekly backups on our cloud every Fridays, as long as it was connected to our internal network, we can assume the latest backup was last Friday evening. So, we do have a backup to restore your data and only work done locally on your machine between Monday and Wednesday before travelling to the conference may be lost. Your hard drive is encrypted, right?”

CEO: “You mean in the exercise or in real life?”

Facilitator: “The hard drive of the stolen laptop was encrypted.”

CISO: “That’s great, but … JJ, what about your real laptop?”

CEO: “Ehm … I was afraid it may slow down performance, so I disabled the encryption a while back.”

CISO: “JJ, we seriously need to have a talk after this … Anyway, for now let’s move on considering that the data is encrypted, and you also have 2FA via your phone OTP so, while we have to assume that all your passwords and the data will ultimately be compromised anyway, we do have some time to update everything and limit further damage.”

Facilitator: “Thanks, Bob. That’s correct. So, while you and JJ work out the inventory of sensitive information that the thief may manage to get access to, I would ask Mary and Jean to start discussing the risk analysis part, assuming a worst-case scenario where the thief manages to access the encrypted data related to our products and clients, as well as establishing a proper communication plan.”

The exercise would then continue with the discussion following the playbook and, implicitly, the NIST framework, guiding the team in a sort of self-discovery of their own procedures and identify possible bottlenecks and oversights that will be addressed in the post-incident review.

Using the MITRE ATT&CK Framework to Articulate Realistic Threats

Another very relevant tool that can be used to design realistic and useful exercises is the MITRE ATT&CK framework [3]. Developed by MITRE Corporation, a well-known nonprofit organization in the cybersecurity world, the ATT&CK Framework serves as a globally recognized repository of adversary tactics and techniques. ATT&CK, an acronym for Adversarial Tactics, Techniques, and Common Knowledge, provides a methodical framework for categorizing and analyzing the methods employed by cyber adversaries across different stages of an attack and can be a very useful tool in a variety of situations, including the design and planning of training exercises due to its encyclopedic nature of categorizing many different attacks and mapping them to real-world scenarios.

At its core, the MITRE ATT&CK Framework comprises a matrix that aligns adversary behaviors with specific tactics and techniques. This matrix is organized into distinct categories, ranging from initial access to impact, each containing numerous techniques catalogued to provide detailed insights into attacker methodologies, as shown in Figure 2.2.

Referring to such techniques would be very important when designing realistic exercises for a more technical audience, including also possible “injects”, a term that is used in the context of a TTX to represent some possibly surprising and unexpected event that adds a twist or additional complications to the existing scenario to move the narrative forward.

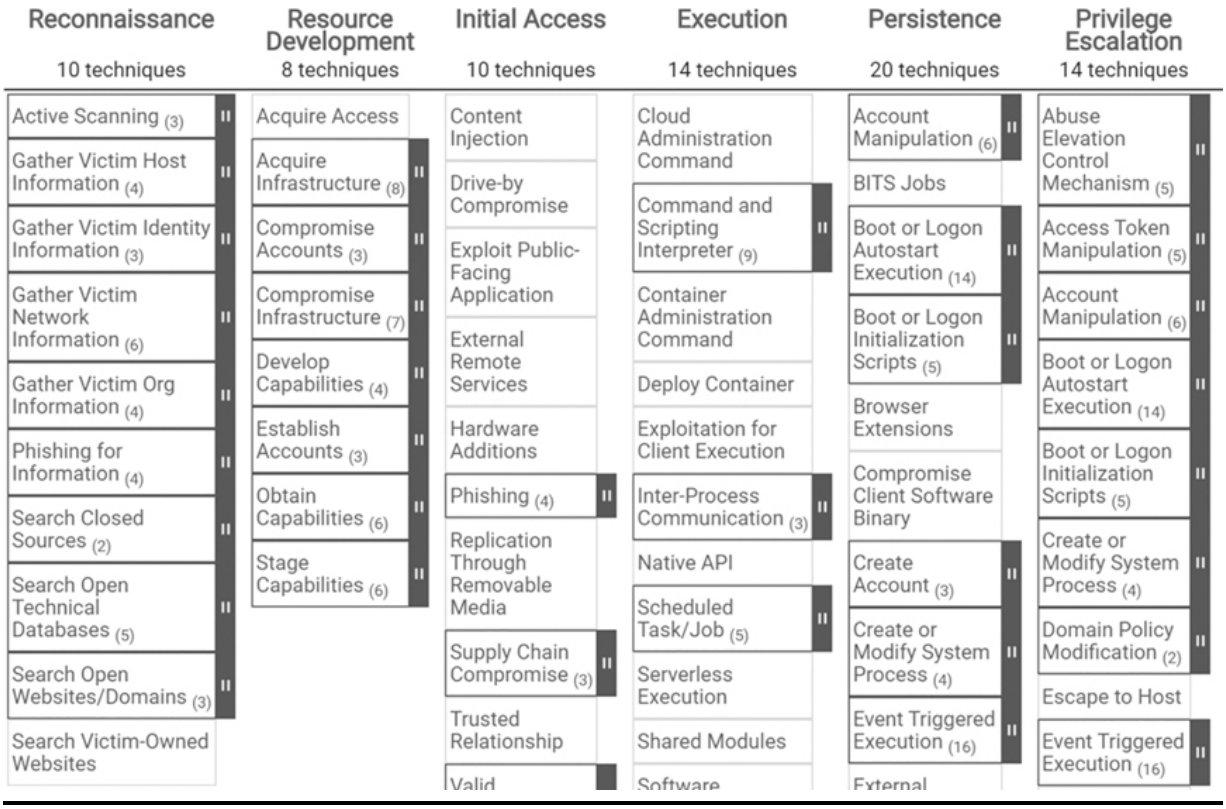

Figure 2.2 A section of the MITRE ATT&CK matrix listing different techniques for different attack phases. On the website, clicking on each technique will link to a dedicated page with additional information, including possible detection and mitigation strategies. ⏎

TTX Example Ⅱ

Now we want to adapt the stolen laptop scenario to a more technical exercise for the IT and cybersecurity teams. In this case, the narrative could begin like this:

Facilitator: "It's Friday evening and you get notified by Bob, our CISO, that JJ's laptop has been stolen at the conference he was attending. The laptop is password protected and data on the hard disk are encrypted. The thief may not even know who JJ is, but we need to assume the worst-case scenario, that is, this was not a random act but our CEO, and our

company, was specifically targeted. What do you think can happen now?”

The team should then start brainstorming different scenarios. If not already outlined in the relevant company’s playbooks, or in the case where the incident is used as a starting point to craft the relevant playbook, resources such as the “attack navigator” [4] provide an invaluable tool to remain focused on actual threats and point out all the possible actions that a determined threat actor could take. After a brief discussion, some of the following possibilities should be pointed out, or “injected” in the narrative by the facilitator if the team can’t find the right thread to move on:

1. **Initial Access:**

    - **Tactic:** Spear Phishing Attachment (T1566.001)
    - **Technique:** An attacker could leverage information obtained from the stolen laptop to craft convincing spear-phishing emails containing malicious attachments. Upon opening the attachment, the recipient’s system could be compromised, providing the attacker with a foothold for further access to information and sensitive company data.

2. **Execution:**

    - **Tactic:** Command and Scripting Interpreter (T1059)
    - **Technique:** The attacker may execute scripts or commands on the stolen laptop to gather additional information, escalate privileges, or establish persistence within the compromised system and network.

3. **Credential Access:**

    - **Tactic:** Credential Dumping (T1003)
    - **Technique:** If the stolen laptop has cached credentials or stored passwords, the attacker could employ techniques to extract these

credentials from the system, granting them access to additional accounts and resources within the organization.

4. **Discovery:**

- **Tactic:** System Information Discovery (T1082)
- **Technique:** The attacker may gather information about the stolen laptop and the broader network environment, identifying potential targets for further exploitation or reconnaissance.

5. **Lateral Movement:**

- **Tactic:** Remote Desktop Protocol (T1021.001)
- **Technique:** With access to the stolen laptop, the attacker could attempt to establish remote desktop connections to other systems within the organization's network, facilitating lateral movement and further compromising additional endpoints.

6. **Collection:**

- **Tactic:** Data from Local System (T1005)
- **Technique:** The attacker could exfiltrate sensitive data stored on the stolen laptop, such as documents, files, or email archives, to gather valuable information for espionage or extortion purposes.

7. **Exfiltration:**

- **Tactic:** Exfiltration Over Command and Control Channel (T1041)
- **Technique:** Once the desired data is collected, the attacker may exfiltrate it from the stolen laptop using established command and control channels, transmitting the stolen information to an external server under their control.

8. **Impact:**

- **Tactic:** Data Destruction (T1485)

- **Technique:** As a final act, the attacker could initiate data destruction operations on the stolen laptop or other systems within the organization's network, causing significant disruption and damage to critical assets and operations.

Whenever multiple threats are discussed, the team should be asked to prioritize them, considering both the possible impact and the timeline (an imminent threat may be prioritized instead of an even more critical one that requires more time to be set up and executed), and then start acting accordingly. This can be decided by the team autonomously or be injected into the narrative by the facilitator if the team is getting confused or misses something important. In our example, the facilitator decides to emphasize the spear phishing risks of the legit email account being abused first, referencing a case of Business Email Compromise (BEC) and the T1566.001 ATT&CK technique. The exercise could continue like this:

Facilitator: "Soon after the incident, a few employees start receiving emails from JJ's original account asking them to check an attached spreadsheet and provide feedback. Some of our partners also receive messages from JJ asking them to update their financial records to a new bank account to be used for all future payments … How shall we mitigate this?"

Team Member 1: "First, we need to log out JJ from every system and server and change his password to a new one so that his email can't be used anymore. Then we need to send an urgent email to all employees and our partners, notifying that JJ's email account was compromised and to delete all messages received after the time the theft took place."

Team Member 2: "I would actually blacklist his email entirely and assign him a new one!"

Team Member 3: "We also need to check all the logs for any activity that came from the laptop to see how it was used and blacklist it, of course."

Note how the exercise here has stepped directly into the "Containment" phase of the NIST framework, to stop the hacker from using the CEO

accounts and identity and do further damage.

As the discussion continues and more practical steps and procedures are outlined and referenced, the facilitator should ultimately lead the session to an end by summarizing any lessons learned. Were all the procedures adopted sound and strong enough to mitigate the risk of real damage, financial, reputational, and so on? Was there any new, practical strategy that was mentioned that could improve the company's current security posture in the future? Even a very simple scenario like the one we just saw may help a team realize they need a more nuanced and effective layered defense in place.

In the end, the outcomes may include the implementation of new advanced email authentication mechanisms such as anomaly detection and behavior analysis to identify and flag abnormal patterns in email communications (e.g., sudden changes in sending behavior or unusual activity in accounts that may have been compromised, like mass distributions of emails in a short time, and so on) or the adoption of tools able to perform email content analysis capable of scrutinizing the content of incoming emails for signs of phishing indicators, including suspicious links, attachments, or requests for sensitive information. Additional endpoint security controls may also be discussed, including endpoint detection and response (EDR) solutions capable of detecting and mitigating suspicious activities, such as unauthorized access attempts or data exfiltration.

If a TTX is able to trigger this kind of discussions, we can affirm the exercise was indeed very successful not only as a tool to check the current procedures and train the staff to follow them in an emergency situation but also as a platform to brainstorm how to improve such procedures and ultimately strengthen the overall company's posture.

Limitations of TTX in a Corporate Environment

An effective TTX is designed to put people under pressure and may also require participants to take hard decisions, or even risking proposing stupid ones, too. This is something that should be welcomed as the whole point of

the exercise is to practice, clarify doubts, and understand possible mistakes so that they won't actually happen later in a real incident. Nonetheless, would participants feel embarrassed if they propose something that others may see as "silly" or useless? Would they feel ashamed if they propose an action that fails to follow a procedure properly? What if they propose something drastic that may annoy their boss, such as suggesting to replace the compromised CEO's email and its straight-forward blacklisting, like it was mentioned in the previous example, so that no new emails can be written from that account at all?

These are concrete possibilities that also need to be considered. After all, this is supposed to be an official training exercise between colleagues in a professional setting, not a weekend afternoon spent playing board games with a group of a tightly knit community of friends!

To avoid these, possibly even subconscious, drawbacks and pitfalls, an RPG-inspired approach may help, and that is exactly what we are going to learn in the remaining part of this book.

References

1. https://csrc.nist.gov/pubs/sp/800/61/r2/final ⏎
2. https://www.isc2.org/Insights/2023/08/effective-board-communication ⏎
3. https://attack.mitre.org/ ⏎
4. https://mitre-attack.github.io/attack-navigator/ ⏎

3

An Introduction to Gamification, Fun, and Role-Playing Games

DOI: 10.1201/9781003606314-4

Ideally, learning and refining new skills should be engaging and fun. In practice, though, that is not often the case. How can we make this happen?

Years ago, the education community was revolutionized by a new, exciting buzzword: “gamification” or, in other words, the application of gaming techniques in a non-gaming context, like learning or corporate training. To some, this looked like a silver bullet to finally make any task more engaging and fun.

Naturally, a word itself means nothing unless its underlying theories are properly understood and translated into a new domain and, unfortunately, an actual “theory of fun” is extremely elusive and cannot be summarized into a mathematical formula, however complex. In fact, not even the most successful game designers really know why their games are so fun to play. Making a successful game is always a very elusive and risky business even for the most experienced people in the industry. It should not be a surprise then to admit that, more often than not, so many “gamified” applications turn out to be much less exciting than expected. In many cases, if we look under the hood of a gamified activity, we will find that only the most trivial aspects of games, that is, the infamous triad of points, badges, and leaderboards were adopted and, often, applied without any real thought.

Rewarding users and giving them a score or ranking to compete against each other are, as we will see, fundamental aspects of games but, by themselves, they are not enough. The reason is that the aforementioned triad consists of the so-called “external motivators”. These are simple external rewards that, by themselves, cannot turn a boring task into a long-term commitment users are eager to undertake. To succeed, the activity needs to engage people at a deeper level by relying on internal (or “intrinsic”) motivators instead. This means that users need to be naturally motivated to engage in the activity not because of some reward or prize, whose effect will soon or later fade and become less relevant, but because they do sincerely (and often subconsciously) enjoy what they are doing.

Ok, this sounds just like a useless definition of “fun” and it does not answer the question of how we can actually achieve such a feat. Essentially, there are two main aspects that are at play here and are a key to a successful engagement.

First, the activity needs to offer a “sense of agency”, that is, users need to feel like their choices matter and have a direct influence on the final outcome. Second, they need to feel a “sense of mastery”, that is, as they put some effort in the activity, they need to notice how their skills are improving and how this helps them to achieve better results. It is important to point out here that this may or may not even be associated to a score or a badge: the realization we can perform a task in a more efficient way, or finding a solution we couldn’t see earlier, are great rewards in their own right and, in many cases, this is what a user is really looking forward to remain committed and engaged.

It is in implementing these aspects, agency and mastery, that successful games do excel. Points and leaderboards are just the tip of the iceberg, a way to make such progress explicit and for all to see, but engagement comes from a deeper level.

To learn how games actually achieve all this, and then see how to replicate such results in our cybersecurity training context, we need first to figure out what players want to have “agency” on, and how they want to express their “mastery”.

Understanding Players and “Fun”

People play games and engage in different activities for different reasons. While each person is looking for a unique experience, by looking at what players try to achieve and focus on during a gaming session, scholars in the field of game studies formulated different models to understand and explain players’ behaviors, enabling game designers to fine-tune their designs so that the resulting games would not disappoint their targeted audience. Among them, Dr. Richard Bartle’s seminal paper “Hearts, clubs, diamonds, spades: Players who suit MUDs”[1] [1] was the first to provide a coherent taxonomy by dividing players engaged in early multiplayer games into four main groups:

- The Socializers, or those who play a game to engage in its social aspects, meet new people and make new friends. For them, a game is a means to an end and not an end in itself. Winning or losing is not necessarily a priority.
- The Killers, on the other hand, need not only to win but also to want the other players to lose. They want to dominate and assert their authority. In other words, they are not dissimilar from a bully.
- The Achievers, or those who want to complete every possible detail of the game, fulfill every sub quest, and get all the rarest items and loot.
- The Explorers, last but not least, play to figure out all the “secrets” of the game. They want to find hidden areas, draw maps, and, maybe, even find novel ways to play and interact with the game systems. Players in this group are hackers at heart and may test a game to its limits!

Since game design is, essentially, all about creating an experience where players can engage with and escape into, these four groups of players tend to look for slightly different types of fun. Indeed, “fun” should not be seen as a single, monolithic abstract concept but can take different forms. Four, to be exact, according to Nicole Lazzaro [2]:

- Hard Fun: this relates to the act of mastering increasingly difficult challenges, often via a trial and error process that takes us progressively towards the desired outcome.
- Easy Fun: this engages players, thanks to visually and content rich environments, with many opportunities for experimentation and interactions with the game world.
- Serious Fun: this manages to engage players by giving an overall meaning to the overall experience. It offers a purpose and a series of goals for players to commit to and focus on.
- People Fun: this relies on social interactions to make the game interesting and allowing for players to bond together and form communities inside and even outside of the game itself.

It should not be difficult to see that the Hard fun is likely what Achievers or Killers may look for. Achievers should also feel highly engaged with Serious Fun, while Easy Fun should resonate well with the Explorers and People Fun is the clear domain of Socializers.

The actual experiences can then take shape in many ways. The important aspect to realize here, though, is that they all happen by engaging players emotionally. The next question then is to identify which emotions are the most important and have a critical role to make players invested in a game. A model that provides an answer to this is the 6–11 Framework, introduced in 2010 in the book “On the Way to Fun” [3].

Here it was proposed that players have a satisfying experience when the game, or activity, manages to arouse one or more basic emotions or instinctive behaviors, which can then interact and support each other to form an engaging whole leading the player towards a “fun” experience.

In particular, the model, as suggested by the name, focuses on six basic emotions and 11 instincts. The emotions considered are the following:

- Fear: one of the most common emotions in games nowadays. Think of any survival-horror games, or dungeon explorations in RPGs, where danger lurks behind any dark corner.

- Anger: a powerful emotion that is often used as a motivational factor to play again or to advance in the story to correct any wrongs that some evil character did.
- Joy/Happiness: arguably, one of the most relevant emotions for having an overall fun gaming experience. Usually this is a consequence of the player succeeding in some task and being rewarded by means of power ups, story advancements, and so on.
- Pride: rewarding players and making them feel good for their achievements is an important motivational factor for pushing them to improve further and advance in the game to face even more difficult challenges.
- Sadness: despite being an emotion that doesn't seem to match with the concept of "fun", negative emotions are also fundamental to make players think on certain themes of the game or on their own performance and learn from their failures.
- Excitement: a game that manages to get players sit on the edge of their seats is a game that has successfully engaged players successfully and got their full attention.

While the list of instincts includes the following:

- Survival (Fight or Flight): the most fundamental and primordial of all instincts, triggered when we, like any other living being, are faced with a life threat. According to the situation, we will have to decide whether we should face the threat and fight for our life or try to avoid it by finding a possible way of escaping. This is widely used in many modern videogames, especially first person shooters (FPS) and survival-horror games.
- Self Identification: people tend to admire successful individuals or smart fictional characters and naturally wish of being like their models and be in their shoes to be the hero of the story and save the world.
- Collecting: a very strong instinct that motivates people to form patterns of objects by completing sets with a common theme. It also

relates to our hunting instinct and has been widely used in games since the early days of the medium.

- Greed: in life, as well as in games, we are often prone to go beyond a simple “collection” of resources and start amass much more than actually needed just for the sake of it. Whether we are talking about real valuable items or just multiple sets of goods we need to build a virtual empire in a strategy game, a greedy instinct is likely to drive many players’ endeavors.
- Protection/Care/Nurture: arguably the “best” instinct of all, and the one that pushes every parent to love their children and every person to feel the impulse for caring and helping those in need.
- Aggressiveness: the other side of the coin, usually leading to violence when coupled with greed or anger. It is exploited in countless of games to satisfy our primordial needs.
- Revenge: another powerful instinct that can act as a motivational force and is often used in games to advance the storyline or to justify why we need to annihilate some enemy.
- Competition: deeply linked with the social aspects of our psyche and one of most important instinct in relation to gaming, for example, leaderboards. Without it, many games would lose much of their appeal.
- Communication: the need for expressing ideas, thoughts, or just gossip was one of the most influential for human evolution and it is used to great effect in games too, while seeking information by talking to a non-playing character (NPC) or while sharing experiences with other players in chatrooms and forums.
- Curiosity: all human discoveries, whether of a scientific or geographical nature, have been made thanks to these instincts that always pushed us towards the unknown.
- Color Appreciation: scenes and environments full of vibrant colors naturally attract us, whether it is an abstract or a photorealistic setting, an artistic use of color can make any scene more appealing and able to capture players’ attention naturally.

If a game manages to trigger appropriate emotions in the player, these will in turn likely trigger some instinct that the player will have to satisfy in the game itself, for example, a scared player will rely on his survival instinct to escape some danger. The goal of surviving the danger will lead the player to the actual “gameplay”, defined as the interactions with the game world and related systems, which are possible by performing specific “actions” in the game according to the rules of the game itself [4].

Essentially, we have just described what a game is, as summarized in Figure 3.1.

As a practical example, let’s look at one of the most famous video games ever developed, Super Mario Bros by Nintendo. By using the previous model, we can describe the game with the following diagram (Figure 3.2).

Here, the player needs to save a princess. The typical “damsel in distress” trope works very well to elicit our protective instincts, giving the motivation to start exploring the game and getting increasingly curious about the game world, its levels, and secrets that, as we uncover them, make the players feel excited and proud of their progress. The addition of power ups to gain additional skills and coins to grab throughout the adventure also manage to trigger our greedy instinct and make players look for even more coins. All together, these build up to create a memorable experience that has engaged generations of players.

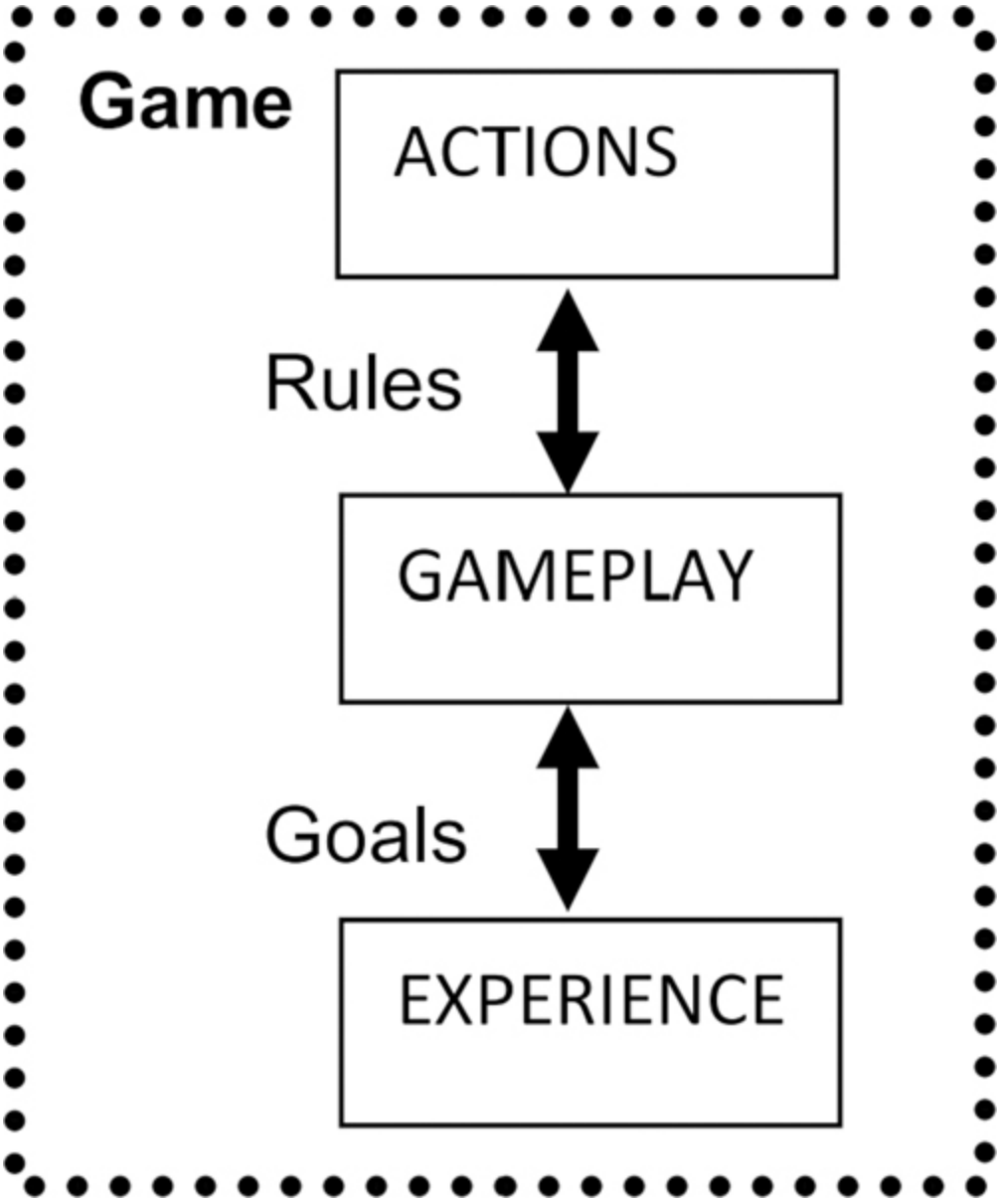

Figure 3.1 Via the AGE (Actions-Gameplay-Experience) framework, we can understand the inner workings of a game by dividing it into three layers. Players do perform some actions according to specific rules, which allow the player to engage with the game context itself to achieve some predefined goal. In doing so, different emotions and instincts are aroused, which engage the player in a meaningful experience. ⏎

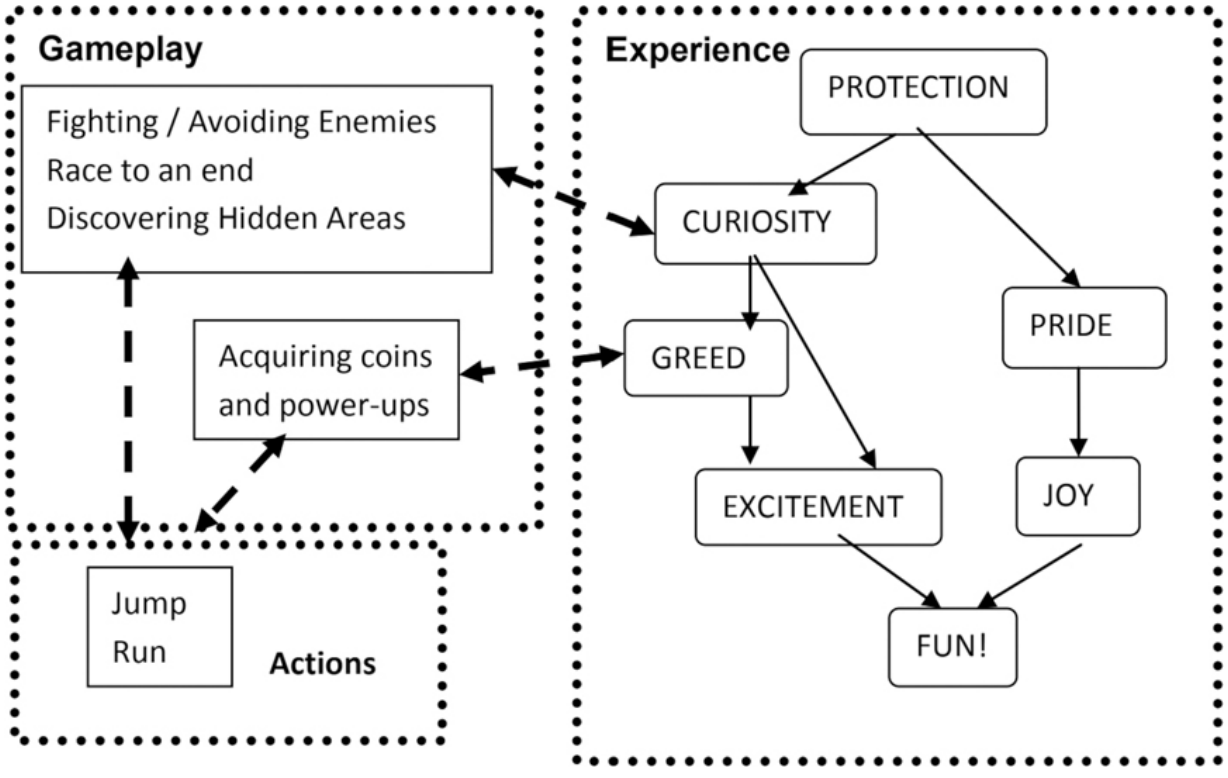

Figure 3.2 A possible analysis of 1985 game "Super Mario Bos" by Nintendo, outlining how the intended emotional experience is tied to its gameplay and the corresponding basic actions a player can perform within the game. ⏎

This analysis model is quite flexible and we can see how the taxonomies previously discussed can fit here to design experiences that are more suitable for certain types of players or fun. For example, "Killers" will look for experiences focused on Survival, Aggressiveness, Revenge, Anger, and Excitement, while instincts such as Collecting, Curiosity, and Pride will be much more suitable to the "Achievers" group. "Social Fun" will need "Self Identification" and "Communication", while "Easy Fun" can rely on "Color Appreciation" to start engaging players effectively.

Now that we are equipped with a better understanding of game design principles, we are ready to figure out the inner workings of RPGs!

The Origins of Role-Playing Games

"Welcome to the land of imagination."

– Gary Gygax (1938–2008)

The origins of tabletop role-playing games are deeply rooted in a varied set of different historical, literary, and cultural influences, which ultimately led to the creation of D&D in the 1974 [5]. To truly understand the enduring appeal of such games, we must first explore how this innovative form of entertainment emerged from two key sources: wargames and fantasy literature.

Before the advent of role-playing games, there was already a thriving subculture centered around board wargames that flourished in the 1950s and 1960s. These games, often involving small armies represented by cardboard tokens, were primarily simulations of historical battles, like campaigns from World War II. Players would painstakingly recreate different conflicts driven by detailed rules for troop movement, terrain effects, and combat outcomes. Wargames were, at their core, a form of structured play that appealed to a specific type of person: someone who valued strategy, planning, and the intellectual challenge of outmaneuvering an opponent. However, these games were limited in scope – they were grounded in realism, focused exclusively on military engagements, and left little room for creativity or narrative.

Before these games become popular, though, in the early twentieth century, another cultural phenomenon had already taken shape. Fantasy literature, thanks to authors such as J.R.R. Tolkien, C.S. Lewis, and Robert E. Howard, captured the imaginations of readers with tales of heroic quests, mythical creatures, and richly detailed worlds that were based on an extensive folklore and traditions. Tolkien's "The Lord of the Rings", in particular, provided an archetype for fantasy storytelling, complete with maps, original languages, and a sense of epic adventures. This body of work planted the seeds for a new kind of imaginative engagement that invited readers to immerse themselves in worlds vastly different from their own and to dream of wielding swords, casting spells, and embarking on perilous

journeys. In other words, the “escapism” component that makes games so appealing became, if possible, even stronger.

It was the synthesis of the highly detailed structure of wargames together with the imaginative depth of fantasy literature that made games such as D&D possible, turning a relatively simple concept into an incredibly engaging experience. In the early 1970s, Gary Gygax and Dave Arneson, two avid wargamers with a shared passion for fantasy stories, began experimenting with ways to bring narrative, a more nuanced agency with the game world as well as more advanced interactions between players, into the wargaming experience. They envisioned a game where players could step into the roles of individual characters rather than commanding entire armies. These characters would have unique abilities, personalities, and goals, allowing players to interact with a fictional world in a deeply personal way. The result was the first edition of D&D, published in 1974 by Gygax’s company, Tactical Studies Rules (TSR).

At its core, D&D was revolutionary because it shifted the focus of play from competition to collaboration and from a simple, straightforward objective to open-ended storytelling. In D&D, one player takes on the role of the GM, also called Dungeon Master (DM), who acts as the game’s storyteller and referee. The other players create characters, each with a unique set of attributes, skills, and motivations, and work together to navigate the challenges and adventures presented by the GM. The game is governed by an extensive combination of rules and dice rolls, but it also relies heavily on the creativity and imagination of everyone involved, with the GM who has to follow and direct the players at the same time, to ultimately make the game world come to life.

So, why has D&D endured so well for 50 years and counting? What is it about this game, and related spin-offs, that has captured the hearts and minds of millions of players around the world? The answer lies in its unique ability to provide a sense of agency and mastery, which are, as we have discussed earlier, the very same principles that underpin successful engagement in activities such as games or gamified experiences. At the same time, the game managed to build a community of enthusiastic people

around the new “hobby”. Achievers, Explorers, and Socializers, three of the four player groups discussed earlier, would, indeed, find themselves perfectly at home in this context.

Let’s analyze these components a little more in depth as these are also the exact features we want to translate later into our cybersecurity training.

First, D&D offered an unparalleled sense of agency. Unlike traditional board games or even video games, where the choices available to players are necessarily constrained by the limits of some pre-designed type gameplay, D&D provided a sandbox environment where anything was possible. Players can negotiate with a sentient enemy instead of fighting it, if they so desire, attempt to solve problems through clever trickery, or pursue deeply personal goals for their characters that might have little to do with the main storyline that was discussed in the official quest document. The GM serves as both a guide and a collaborator, adapting the game to the players’ decisions and ensuring that their choices have meaningful consequences. This level of freedom is rare in any form of entertainment, and it’s one of the reasons why D&D and other tabletop RPGs remain so compelling to this day.

Second, D&D provided a sense of mastery that goes beyond the improvement of dice-rolling skills or rule memorization. As players progress through the game, their characters gain experience points (XP) and become more powerful, unlocking new abilities and facing greater challenges. But mastery in D&D is not just about mastering rules and gaining abilities to face stronger monsters; it’s also about storytelling and about “what if” scenarios. Players learn to think creatively and out of the box, solve problems collaboratively, and express their characters in nuanced ways. This progression mirrors the journey of a hero in a story, creating a satisfying arc of growth and a sense of accomplishment.

Finally, the focus on team building, where the abilities of each player complement those of the other members of the playing party, foster a sense of community that is integral to its continuous success. At its heart, D&D is a social game. It requires players to come together not just for a single stand-alone game but for epic quests that can last over weeks or even

months and share a collective experience that will be fondly remembered for a long time. The bonds formed around the gaming table, whether physical or virtual, are often as important as the game itself. Players laugh together at unexpected outcomes, mourn the loss of beloved characters, and celebrate hard-won victories. This sense of camaraderie is a powerful draw, especially in a world where opportunities for genuine social connection can sometimes feel scarce.

The enduring success of D&D teaches us some very important lessons about how to build successful engagements: the desire to tell stories, to explore new worlds, and to connect with others in meaningful ways is something we are naturally drawn to. It is a game that celebrates creativity, collaboration, and imagination, that, nevertheless, is built on a very solid foundation with extensive rules and game systems that enable such creativity to arise naturally and lead players across a treacherous and unpredictable world. It is now time to look into such systems in more detail.

The Inner Workings of an RPG

By using the analysis model outlined earlier, we can represent a generic RPG in the following way (Figure 3.3).

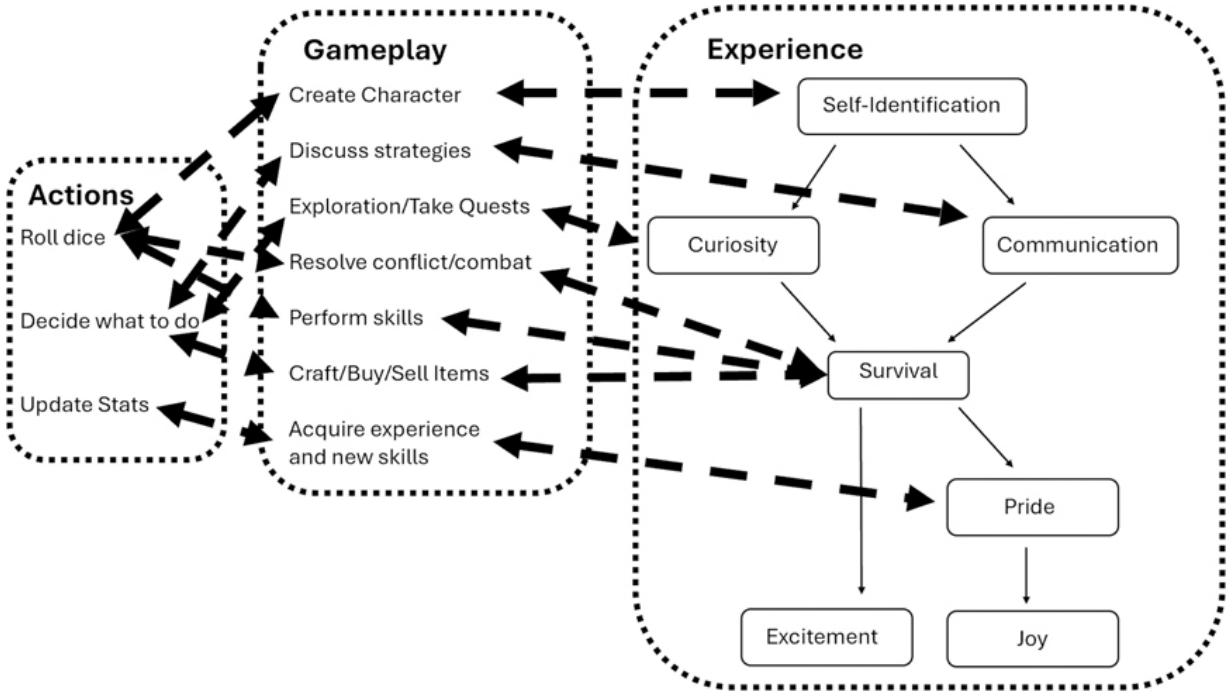

Figure 3.3 A possible analysis of a typical RPG according to the AGE and 6–11 frameworks. Basic but very flexible actions allow for a complex gameplay involving several game sub-systems, from conflict resolution to character outfitting and progression which are achieved via the acquisition of XPs and new skills. These, in turn, allow for a truly immersive experience centered around our curiosity, communication, and survival instincts. ⏎

Such an engaging experience can only be delivered by a strong sense of self identification: players must feel they are in the heroes' shoes. RPGs are able to deliver this aspect very effectively from the get-go via a character creation process that allows players to customize their character extensively by choosing different races and roles with distinct abilities and traits. Communication among the participants is paramount, as it is a growing sense of curiosity to explore the fantasy world to find out all the challenges and secrets it is hiding. Once the adventures start, dangerous situations will naturally happens, forcing players to take important decisions to survive and help each other.

The gameplay includes the implementation of several systems that we need to understand if we want to later translate a similar experience into our cybersecurity context. In particular, we need to explore the following:

- Conflict Resolution
- Character Creation
- Progression and Rewards
- The Art and Science of Quest Design

Conflict Resolution

In role-playing games, the heart of the experience lies in the players' ability to interact with the game world in meaningful ways. Whether they are negotiating with a king, sneaking past a group of guards, or battling a fearsome dragon, players constantly face challenges that require to be assessed and resolved. This process, known as "conflict resolution", is essential to the progress of the game. It determines what happens when players attempt to do something, especially something with an uncertain outcome. Understanding how conflict resolution works is key to understanding how role-playing games function. Let us use D&D as our main reference to explore these systems and explain them in simple terms.

At its core, the conflict resolution system in D&D is a framework for determining the success or failure of a player's actions. The process typically involves three main components: the player's intent, a set of resolution rules based on a mix of stats and luck, and the consequences of any action performed according to such rules. Each of these components plays a vital role in shaping the narrative, maintaining fairness and consistency across the game.

The first step in any conflict resolution is the player's declaration of intent. This is where the player describes what their character is trying to do. For example, a rogue might say, "I want to pick the lock on the treasure chest", or a fighter might declare, "I swing my sword at the goblin". This step is crucial to set the stage for what happens next. The GM listens to the player's intent and decides whether the action is feasible within the specific

context. In many cases, the GM will also ask for additional details to clarify the player's approach. For instance, if a player wants their character to persuade a guard to let them pass, the GM might ask, "What do you say to the guard?" or "How do you approach them?" This encourages players to think creatively and role-play their actions, adding depth to the experience.

Once the intent is clear, the next step is to determine whether the action succeeds or fails. In D&D, this is usually done through a combination of character abilities like dice rolls and rules.

Each character in D&D has a set of abilities, such as Strength, Dexterity, and Intelligence, which represent their natural talents and capabilities. These abilities are given numerical scores, usually across a range between 1 and 20, which reflect how good the character is in each area. For example, a character with a high Strength score is better at physically demanding tasks like lifting heavy objects or breaking down doors, while a character with high Dexterity is more agile and skilled at tasks like sneaking or dodging.

In addition to abilities, characters often have specific skills that further represent their qualities. These skills, such as Stealth, Persuasion, or Arcana, are tied to the abilities and provide bonuses to related tasks. For instance, a rogue with training in Stealth will be better at sneaking past enemies than a character without that skill.

But skills alone are not everything. Knowing we are good at something is not a guarantee to success and the outcomes in the game are kept open so as to have an experience that is always exciting: a strong player may still fail while a weak one may still have hope to escape a dangerous and apparently hopeless ordeal.

The outcome of an action is usually determined by rolling a 20-sided die (commonly called a d20). This roll is the cornerstone of D&D's, as well as most other RPGs, conflict resolution system. The player rolls the die and adds any relevant modifiers from their character's abilities and skills so that relevant acquired expertise can help in achieving the desired outcome. The total result is then compared to a target number, known as the Difficulty Class (DC), which is set by the GM based on how hard the task is supposed to be. For example:

- Picking a simple lock might have a DC of 8 (easy), meaning that if we roll at least an 8 we will be successful.
- Convincing a skeptical guard to let you through might have a DC of 13 (moderate).
- Leaping across a collapsing bridge might have a DC of 18 (hard, as it will likely require a good roll as well as a certain amount of bonus points from the player's skills).

If the player's total equals or exceeds the DC, the action is successful. If it falls short, the action fails. This simple mechanic creates tension and excitement, as players never know for sure how their attempts will turn out. It should also be noted that, to keep doors always open for potential surprises, a rolling a straight 20 will always be a success, while rolling a 1 will always represent a failure.

When we get to combat, this is just a special kind of conflict resolution with its own set of rules. When a character attacks an enemy, the player first rolls a d20 to see if the attack hits. This roll is compared to the enemy's Armor Class (AC), which represents how hard they are to hit. If the roll equals or exceeds the AC, the attack is successful, and the player then rolls additional dice to determine how much damage the attack deals, according to the specific weapon they are attacking with.

Combat also incorporates other factors, such as initiative (to determine turn order), movement (to position characters on the battlefield), and special abilities or spells. These elements add layers of strategy and complexity to combat, making it one of the most engaging parts of the game.

Finally, this approach is also used for determining consequences of any other possible action. Whether the player's attempt succeeds or fails, the outcome should have an impact on the story. For example:

- If a rogue successfully picks the lock that had a DC equal to 0, then they might find a cache of treasure or a critical piece of information inside the chest.

- If a fighter misses their attack, the goblin might retaliate or attempt to flee, creating new challenges for the party.
- If a wizard's persuasion skill fails to convince the guard to let them pass, the party might have to find an alternate route or devise a clever plan to sneak past.

In some cases, an unlucky roll can also lead to exhilarating complications that propel the story forward. For instance, a failed stealth attempt might alert nearby enemies, leading to an unexpected combat encounter that can provide additional rewards.

It should be noted that, while predefined challenges may have scripted outcomes, players with a vivid imagination may quickly go astray and try very original solutions to certain situations, forcing the GM to improvise. This is exactly where the GM's role as a storyteller truly shines and makes an RPG gaming session with a group of old friends a truly dynamic and memorable experience for everyone involved. Two playing sessions are never the same.

The lesson to learn here from D&D's conflict resolution system is in its balance of structure and flexibility. The rules provide a clear framework for determining outcomes, ensuring fairness and consistency, while still leaving room for creativity and improvisation. Players feel a sense of agency because their choices and actions directly influence the story, and they experience a sense of mastery as they learn how to navigate the rules and develop strategies for success.

Character Creation

In the previous section, we mentioned wizards, rogues, and other fantastic types of heroes and foes. Indeed, one of the most exciting aspects of role-playing games is creating a unique character that will serve as our alter ego in the game world. This process, known as "character creation", is the foundation of the game experience. It allows players to craft unique individuals, complete with strengths, weaknesses, and personality traits, who will interact with the story and the game world in unique ways

following the players' directives. Most importantly, in doing so, players will naturally feel invested in their creations, and the self-identification instinct, which is often fundamental for creating an engaging experience as we saw earlier, will be very strong and completely natural.

For these reasons, RPGs take great care in the character creation process, making sure it is both highly structured and flexible so that players can create characters tailored to their personal preferences and playing styles. When creating a new hero, players first need consider a few key questions: Who is the character? What can he or she do? And how do they interact with the world around them? To answer these questions, the game uses a combination of rules and narrative elements. The former includes stats and abilities that define what your character can do, while the narrative side focuses on the character's backstory, personality, and motivations.

From a practical perspective, the process begins by choosing two fundamental aspects of the new character: their "race" and their "class". Race, for example, human or elf, determines the character's physical traits, such as height, appearance, and special racial abilities, while class defines their role in the game, such as a fighter, wizard, or rogue. Together, these choices provide the foundation for a character's identity and capabilities and set up the stage for a particular style of gameplay. Once a player has chosen the character's race and class, the next step is to determine the core stats, also known as "ability scores". These are the fundamental attributes that define a character's strengths and consequent weaknesses. For example, common ability scores include:

- Strength: measures physical power and athleticism. This is important for characters who rely on brute force, such as warriors, fighters, and similar.
- Dexterity: represents agility, reflexes, and balance. It's crucial for characters who rely on precision, like rogues and rangers.
- Constitution: reflects endurance and resilience. A high Constitution score means the character can take more damage and recover from injuries more easily.

- Intelligence: indicates reasoning and knowledge. Wizards and other scholarly characters need a high Intelligence score much more than a fighter.
- Wisdom: measures perception and insight. This score is a key for characters like clerics and druids, who rely on their understanding of the world and their intuition.
- Charisma: represents charm and social skills. Characters like bards and sorcerers may use Charisma to influence others and cast spells.

These ability scores are determined during character creation, usually by rolling multiple six-sided dice (D6). Each score is assigned a number within a 20 points scale, typically ranging from 3 (very poor) to 18 (excellent), and these numbers are translated into modifiers that influence the outcomes of dice rolls during the game. For example, a character with a high Strength score will receive a bonus to rolls involving physical feats like lifting or breaking objects.

Earlier we mentioned different races. Specific choices in this regard also do affect the character creation process significantly, as each specific choice comes with its own unique traits and abilities, adding depth and flavor to the character being developed. For example, typical races a player can choose include:

- Elves, known for their grace, agility, and keen senses. They often receive bonuses to Dexterity and have special abilities like heightened perception or resistance to magical effects.
- Dwarves, strong and resilient, with bonuses to Constitution and abilities that make them resistant to poison and skilled in working with stone and metal.
- Halflings, also known as “Hobbits” and typical of Tolkien’s epic stories. They are small and nimble, traits that grant them bonuses to Dexterity and extra chances in critical situations.
- Humans, versatile and adaptable, with balanced stats that allow them to perform well in any role.

These racial traits provide specific advantages in the form of certain stats boosts and bonuses and, henceforth, help define a character's unique place in the world. They also interact with the chosen class to create a wide range of possibilities and unique combinations. Classes, in fact, determine a character's default role in the game and the corresponding primary abilities. Similar to races, each class has its own strengths, weaknesses, and natural playing style. Typical classes common across most RPGs include the following:

- Fighters: they are masters of combat. Fighters rely on Strength or Dexterity to excel in battle. They can wield a wide range of weapons and wear heavy armor, making them versatile and very resilient.
- Wizards: spellcasters who draw on their Intelligence to learn and cast powerful spells. Wizards are fragile but incredibly versatile, capable of manipulating the battlefield and solving problems with magic.
- Rogues: agile and cunning, rogues rely on Dexterity and specialize in stealth, deception, and precision attacks. They're excellent at navigating traps and dealing with enemies from the shadows.
- Clerics: they are holy warriors who usually rely on their wisdom to heal allies and smite foes. Clerics are versatile, with access to both offensive and defensive spells, and are usually fundamental in keeping a party alive.

Each class comes with unique abilities and features that, when coupled with the traits of each race, can give birth to unique combinations. In fact, the interaction of race, class, and ability scores allows players to create characters with distinct play styles that perfectly integrate and complement each other for the overall benefit of the party. A high Strength score might suit a knight who charges into battle headfirst, while a high Charisma score might be perfect for a bard who wants to persuade and inspire others. Similarly, a high Intelligence score could make a wizard an expert at solving puzzles and uncovering secrets.

The freedom offered by such a system is perfect to encourage players to think creatively and experiment in novel and original ways. Moreover, the stats and abilities determined during character creation directly influence the conflict resolution systems discussed earlier. When a player attempts an action, the relevant ability score, plus any related modifiers due to items or bonuses, is used to determine the outcome. Let’s illustrate this with a couple of examples:

- If a fighter wants to shove an enemy, they might make a Strength check, adding their Strength modifier to the roll and see if the final results beats the target decided by the GM.
- If a rogue tries to sneak past a guard, they’ll make a Stealth check, which is based on their Dexterity and any bonuses from special training or racial traits.
- If a wizard attempts to decipher an ancient text, they’ll make a Knowledge or Arcana skill check, which uses their Intelligence modifier.

In combat, these stats also play a crucial role. Attack rolls are based on Strength or Dexterity, depending on the weapon, while spellcasters use Intelligence, Wisdom, or Charisma, according to the rules of the specific RPG being played, to determine the effectiveness of their spells. Hit points, which represent a character’s ability to withstand damage, are influenced by Constitution.

To get a better understanding of how all works in practice, let’s take a closer look at how a newly created character’s stats are designed to give players a fair chance in the game. Suppose a player creates a human fighter. By rolling 3D6, for example, we could get a Strength score of 16 (providing a +3 modifier, assuming a common rule that assigns a bonus equal to the roll minus 10 and then divided by 2) and a Dexterity score of 12 (providing a +1 modifier). This character is well-suited for melee combat but has some versatility for ranged attacks or dodging. The GM then describes a scenario where the fighter must break down a locked door to rescue a trapped

villager. The GM asks for a Strength check, setting the difficulty at 14. The player rolls a d20 and gets a 12. Adding the +3 modifier from their Strength score, the result is 15, a success! The door splinters under the fighter's might, and the villagers cheer.

Next, the party is ambushed by goblins, and the fighter engages in combat. The fighter attacks with their sword, rolling a d20 to hit. The goblins have an AC of 13. The player rolls a 10 but adds the +3 Strength modifier for a total of 13, just enough to land a hit. The fighter's sword deals damage based on a roll of an eight-sided die (d8), plus the Strength modifier, ensuring the goblins are swiftly dealt with.

These examples highlight how ability scores and modifiers ensure that even new characters have a reasonable chance of success. Most tasks and combat rolls fall within the 1–20 range, allowing players to contribute meaningfully to the game even at low levels. The combination of stats, modifiers, and dice rolls creates a balanced system that rewards effort while keeping outcomes uncertain and exciting.

While the technical aspects of character creation are important, the narrative side is equally vital to build an engaging experience and make players invested in the game and their alter ego. Players are encouraged to think about their character's backstory, personality, and goals. Why did they choose their class? What drives them to adventure? These elements bring characters to life and create opportunities for role-playing and storytelling. A player might decide that their dwarf cleric is a devout follower of a god of justice, seeking to cleanse corruption wherever they find it. Or they might decide that their mischievous bard is a charming trickster, who uses music to mask a troubled past. These details provide hooks for the GM to weave lots of original elements into the story and help players connect with their characters at a level that no other game can match.

Progression and Rewards

No game (or activity) can manage to build an engaging experience without giving its participants a sense of growth and achievement. In the case of

RPGs, this growth is primarily realized through the process of gaining experience, progressing across levels, and receiving rewards. The interplay between these elements forms a crucial part of what makes these games so satisfying. Let's delve into this area to understand how it actually works.

The mechanism of XPs is central to most RPGs as XP serves as a tangible representation of a character's growth. When players overcome obstacles, defeat enemies, or achieve significant milestones within the game, their characters earn a certain amount of XP directly proportional to the difficulty of the challenge they had to face. This accumulation is akin to gaining wisdom and practical knowledge from the character's in-game adventures.

Consider a fledgling wizard who has just completed a dangerous quest to recover an ancient tome from a goblin-infested cavern. For defeating the goblins, bypassing traps, and retrieving the book, the character earns XP, bringing them closer to the next level. Each encounter, whether combat or problem-solving, reinforces the idea that growth is earned through effort and cleverness, giving players a sense of increased mastery, besides the feeling of pride for having overcome some challenging obstacle. Most importantly, once a character accumulates enough XP, they "level up", marking a significant step in their journey. Leveling up grants various benefits depending on the game's system. In D&D, for example, it might mean gaining more hit points (a measure of resilience), new abilities, like additional spells for a wizard, or enhanced proficiencies, opening up new opportunities and options so that players feel their choices and efforts had a direct impact on their character's progression, feeding, once again, into that critical sense of mastery.

While XP and leveling are foundational and provide a straightforward measure of a player's progression, the rewards players seek often go deeper. Players are motivated by what Neal and Jana Hallford categorized as the four types of rewards in their seminal work "Swords and Circuitry" [6]. Let's break these down and see how they shape the RPG experience.

First, there is the "Rewards of Glory". These are the intangible yet deeply satisfying rewards that players carry with them beyond the gaming table.

They include moments of triumph, such as defeating a powerful dragon or completing a grueling campaign. These experiences fuel players' pride and sense of accomplishment. For example, let's imagine that, after several sessions of meticulous planning and daring action, a party of adventurers finally vanquishes a dragon threatening the kingdom. The victory isn't just about the XP or treasure earned – it's about the story they've created and the memory of the teamwork and courage it took to succeed.

Then we have the "Rewards of Sustenance". These are the practical rewards that keep characters alive and functioning. Typically, these might include health potions, scrolls, or mundane gear like ropes and torches. While not flashy, they are indispensable and can have a significant impact during a quest. Imagine a rogue running low on hit points after a skirmish with bandits. A healing potion found in the bandit leader's treasure hoard can be the difference between life and death. Sustenance rewards provide a safety net, ensuring players can continue their adventures despite setbacks.

The next category includes the so called "Rewards of Access". These rewards unlock new possibilities by granting access to previously unreachable areas or resources. A key to a locked dungeon door, a magic password to an ancient library, or even a map revealing hidden locations are prime examples. Let's return to our wizard. Suppose the party acquires a rare magical amulet that allows entry into a long-sealed tower. The tower, rumored to contain forbidden knowledge and powerful artifacts, opens a new chapter in the game. Such rewards excite players by expanding the scope of their adventures, making them feel they are uncovering secrets and blazing new trails.

Last, we have the "Rewards of Facility". This group of rewards empowers characters to do things they couldn't do before or enhance existing abilities. These include magic items and spells, skill upgrades, or new, more powerful weapons. When properly implemented across the game, these rewards enrich gameplay by increasing the player's strategic options and can be very effective when granted at the end of a quest, to prepare for the next challenge, or just before a climactic battle. As an example, consider a ranger who finds a bow imbued with magical energy.

This bow might allow the ranger to shoot twice as far or inflict extra damage on undead foes. Suddenly, combat encounters involving undead become more engaging, as the player can exploit their newfound advantage. It should also be noted that facility rewards often align with the concept of building a skill tree. As players progress, they choose abilities or upgrades that suit their preferred playstyle, reinforcing, once again, a sense of agency and mastery.

To recap, let’s tie this together with an example that incorporates XP, leveling, and rewards. Imagine a group of adventurers, for example, a wizard, a rogue, and a ranger, who are on a quest to explore a cursed temple. Suddenly, the party faces a group of skeletons guarding a treasure chest. Each player performs an attack roll by throwing a D20 and compares the result with the AC of the selected enemy to determine whether the attack strikes or not. The ranger rolls a 16, hitting a skeleton and dealing a certain amount of damage. The rogue tries to sneak past an enemy but he is discovered and is attacked, luckily he rolls a 12 and successfully dodges the incoming blow. The wizard, unfortunately, rolls only a 4, failing to cast “Magic Missile”. After a few more rounds, the party is victorious and earns 300 XP collectively, distributed among the three characters and they find a hidden chest, revealing a “Potion of Healing” (a Reward of Sustenance), ensuring they can recover from any injuries they sustained, a “Skeleton Key” (a Reward of Access), which unlocks a secret door deeper in the temple, and a “Ring of Protection” (a Reward of Facility), granting a +1 bonus to the wearer’s AC. Later, upon leveling up, the wizard selects *Fireball* as a new spell, significantly enhancing their offensive capabilities and making it even easier to cast and avoid embarrassing failures like the one in the previous battle. This choice of rewards by the original game designer exemplifies how leveling and facility rewards together can create a richer and more reliable character.

It is important to understand how RPG progression systems manage to balance short-term and long-term gratification. XP and leveling provide a clear path of growth, while rewards cater to both immediate needs and future ambitions. Glory rewards keep players emotionally invested,

sustenance rewards ensure survival, access rewards expand the game's horizons, and facility rewards deepen strategic possibilities. Together, these elements create a feedback loop of engagement and satisfaction. Players are motivated to push forward, not just for the sake of their characters but for the joy of discovery, the thrill of mastery, and the stories they craft along the way.

The Art and Science of Quest Design

All the different aspects of RPG design we saw in the previous sections offer us a reliable framework to understand how this type of games work. Nonetheless, in the end, all these would be meaningless without an actual quest for the players to engage in, that is, the actual adventure that drives the story forward and engages players in the shared experience of discovery, challenge, and triumph as we discussed so far.

The first step to craft a well-designed quest is to realize how this is more than just a series of tasks following each other. On the contrary, it should be seen as a dynamic narrative playground where the players' skills, abilities, and creativity are given a chance to shine via unexpected possibilities and interactions. Designing such quests is a delicate balance between structure and improvisation, requiring careful consideration of player abilities, pacing, and the role of the GM who will bring it to life as the players' guide, referee, and collaborator.

So, how shall we design such an unforgettable adventure? Exactly like all well-designed story, a quest should also begin with a clear objective, or "hook", that compels the players to act. This could range from rescuing someone in danger to exploring a mysterious dungeon. Along the way, players encounter a mix of challenges, such as puzzles, combat encounters, and moral dilemmas, all leading to a climactic resolution, again following the basic principles of storytelling, but with every single aspect of the adventure fine-tuned to align with the players' abilities. Challenges should feel achievable yet demanding, encouraging players to use their skills creatively and offering meaningful choices with actual consequences. Let's

not forget that players must always feel like their actions matter. Indeed, the most memorable quests are those where players feel their characters' abilities are vital to success. It is important here to note that the original quest designer may have only a general idea of the skills and strengths of the players, who will later engage with his story. Therefore, in practice, it is up to the GM to carefully tailor the original challenges to the actual players' skills, stats, and playstyles. The GM has the right, and some may even say the duty, to update, fine-tune, or even change the original requirements for a given situation so as to make the overall experience better for the current players, by scaling and modifying challenges accordingly.

Nonetheless, as mentioned, a good quest should not just be a series of challenges tied together by some basic story and plot twist. It should have a natural rhythm that alternates between moments of tension and relief. Overloading players with constant danger or puzzles can lead to fatigue, while a lack of challenges risks disengagement. For instance, after a harrowing combat encounter, the GM might provide a quieter moment for role-playing or exploration involving less action-oriented skills. Perhaps the adventurers find a peaceful clearing where they can rest, heal, strategize or meet an interesting character, who can offer rare merchandise or information. These lulls allow for character development and for a deeper understanding and reflection on the game world, increasing the players' emotional investment in the story. In other words, while a quest begins with a scripted plan, the unpredictable nature of RPGs means that flexibility is not only required but it is essential to the game itself. Players are notorious for finding unconventional solutions or wandering off the beaten path, and it's the GM's job to adapt to these moments without derailing the story. For example, take a scenario where the players need to infiltrate a villain's fortress. The GM may have planned for a stealth-based approach, but the players decide to disguise themselves as traveling merchants instead. An inexperienced and rigid GM might insist they stick to the original plan, but a more experienced GM would enthusiastically embrace the unexpected opportunity, creating novel options and challenges for role-playing and skill checks that still align with the original quest's objective.

Improvisation also allows for reactive storytelling. If the players fail a key skill check, the GM can introduce consequences that propel the narrative forward instead of bringing it to a halt. For instance, if the rogue fails to pick a lock, the noise might attract a guard, leading to an impromptu combat encounter or a tense negotiation, after which the party may be able to finally retrieve the key to open the required passage. In other words, the best quests are exactly the right tool to provide players with a sense of agency, where their decisions shape the outcome of the story by presenting dilemmas or branching paths that force players to weigh their options carefully. As an example, consider a quest where the players must recover a stolen relic from a band of mercenaries. Along the way, they discover the mercenaries stole the relic out of need, to ransom their kidnapped families from a corrupt feudal lord. The players now face an interesting choice with moral ramifications:

1. Confront the mercenaries to retrieve the relic directly as originally intended.
2. Side with the mercenaries and investigate the lord and expose his wrongdoing.
3. Negotiate with the mercenaries to find some other peaceful resolution.

Each option has consequences, shaping the story and the players' relationships with the world's characters. By allowing players to make meaningful choices, the quest becomes a collaborative narrative rather than a linear script and the resulting game truly comes to life.

Last but not least, proper quest design should also not lose sight of the more mundane aspects of the game, like satisfying the players' needs for gratification via the type of rewards we discussed previously. There should be plenty of options to find or acquire healing potions or rations to support survival, keys or maps to open new areas or opportunities, magical weapons or skill upgrades that enhance characters' abilities, besides the implicit satisfaction of completing the challenging adventure and overcome all the adversities and obstacles on the players' path.

Let’s bring these principles together with a simple quest: the players are tasked by the mayor of the capital city to retrieve a stolen crown, a thousand year old holy relic and symbol of unity for the whole nation, from a gang of thieves operating in the city sewers. The quest will include details for different types of challenges, and it could progress as follows:

1. As the players approach the sewers, they are potentially ambushed by a group of thugs guarding the entrance. A mix of stealth and combat skills can be used to bypass or defeat them. If the thugs are defeated, players may be rewarded with a map of the sewers.
2. Once in the sewers, the players find a locked gate with a riddle engraved on it. Solving the riddle (or picking the lock) allows them to proceed. Multiple failed attempts may prompt the appearance of a strong guardian, who, once defeated, would provide the much needed key to progress.
3. The following labyrinthine sewers would require expert navigation skills or the map that the players may have found earlier if they fought the goons at the entrance. Scattered healing potions and a few coins lost by previous adventurers would offer some variety and small rewards while a few fights here and there would also be included to keep players on their toes.
4. Ultimately the labyrinth would lead to a final boss encounter and the possibility to retrieve the stolen artifact.

   Notice here the many opportunities for improvisation offered by the original quest, which is, essentially, a canvas that can be fleshed out and customized as the adventure progresses. By doing so, the quest is accessible to a wide variety of players with different skills, and it also offers the GM opportunities to “spice things up” further by including “injects” or additional unexpected events, which force players to suddenly change their strategy or consider new possibilities. If players decide for unconventional approaches and request for something totally unexpected like, for example, bribing the final boss instead of fighting him, what should happen? The GM can adapt, of course, and

create new complications, such as a rival gang hearing of their actions to provide additional challenges for the team to confront with before they can go back to the city and deliver the crown to the mayor.

Note

1. MUD: Multi User Dungeons ⏎

References

1. Bartle, R. (1996). Hearts, clubs, diamonds, spades: Players who suit MUDs. *Journal of MUD Research*, 1(1) (pp. 1–27). ⏎
2. Lazzaro, N. (2012). Why We Play: Affect and the Fun of Games – Designing Emotions for Games, Entertainment Interfaces, and Interactive Products. In *Human Computer Interaction Handbook* (pp. 725–747). CRC Press. ⏎
3. Dillon, R. (2010). *On the Way to Fun*. AK Peters. ⏎
4. 4. Dillon, R. (2014). Towards the definition of a framework and grammar for game analysis and design. *International Journal of Computer and Information Technology*, 15 (pp. 188–193). ⏎
5. Appelcline, S. (2014). *Designers & Dragons: The ‘70s*. Silver Spring, MD, Evil Hat Productions. ⏎
6. Hallford, N. & Hallford, J. (2001). *Swords and Circuitry*. Prima Tech. ⏎

4
PUTTING THE RPG INTO THE TTX

DOI: 10.1201/9781003606314-5

In Chapters 1 and 2, we discussed what TTXs are and why they should be considered as a core component in preparing ourselves for future cyber incidents. In Chapter 3, we got a foundational understanding of game design, gamification, and RPGs. Finally, in the present chapter, it is time to bridge the gap between these two apparently far domains and see how we can design better and more engaging training experiences.

First, in Table 4.1, let's compare TTXs and RPGs:

We can appreciate clear similarities between the way TTXs and RPGs are organized. Both require a team made by people covering specialized roles to solve problems creatively and are coordinated by someone who handles the narrative based on specific materials, whether this is a fantasy quest or a practical cyber incident. Besides this practical comparison, it would also be interesting to discuss a TTX under the lenses of the 6–11 Framework like we did for a typical RPG in Figure 3.3. See Figure 4.1.

As we know, in a TTX scenario, the participants meet to discuss a specific incident with the purpose of discussing the possible strategies and solutions they can implement. To achieve this, they must review existing procedures and debate (i.e., the "Actions") the best possible strategy, deciding the next steps to move forward and, possibly, identify any weakness or holes in their existing security posture (i.e., the "Gameplay"). The specific TTX scenario supports our desire to communicate ideas and

solutions as well as our curiosity to find out what is going to happen next and how the situation would unfold as a consequence of choosing a certain approach. In the end, our decisions, if successful, would make the participants feel accomplished for having managed the case successfully (i.e., the "Experience"). On the other hand, it has to be noted that the purposes, environments, and participant mindsets, do differ significantly between the two activities.

Table 4.1 A direct comparison between TTXs and RPGs ⏎

	TABLE-TOP EXERCISES (TTXS)	ROLE-PLAYING GAMES (RPGS)
Participants	A team of professionals	A party of friends
Coordinator	Facilitator	Game Master (GM)
Materials	Incident Response Plan (IRP), Specific Playbooks	Rulebooks, Character sheets, Dice
Topic	Cyber Incidents	Fantasy Quests

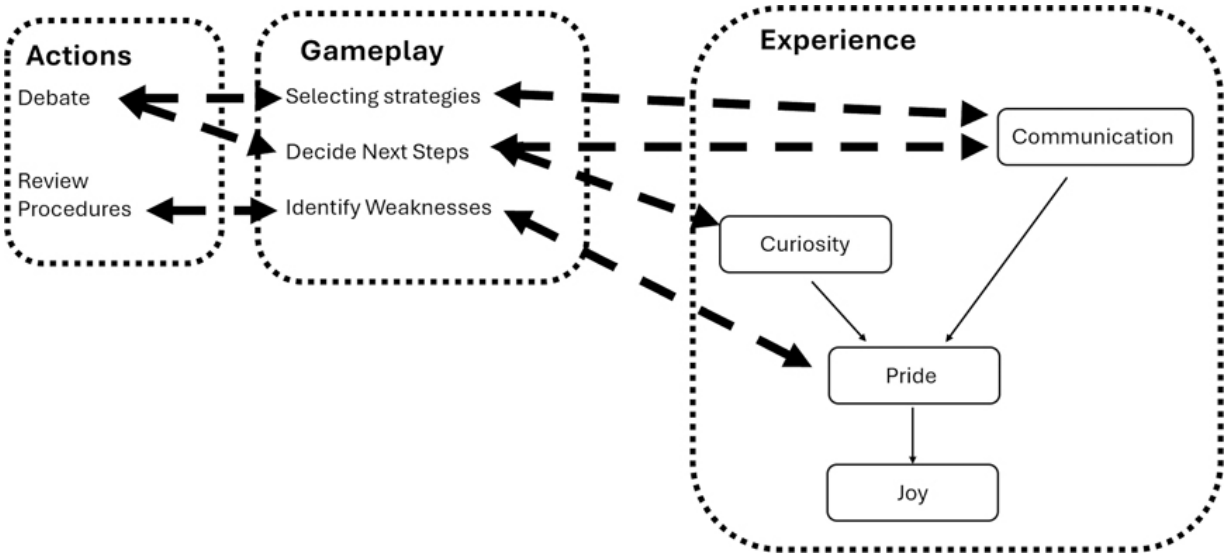

Figure 4.1 AGE analysis for a typical TTX, outlining standard Actions, Gameplay, and resulting Experience. ⏎

Let’s start with the purpose. RPGs are inherently recreational, designed for fun and creative storytelling. Players willingly immerse themselves in fantastic worlds, eager to experiment, take risks, and embrace challenges. Success and failure are part of the narrative experience, and even mistakes contribute to the story’s richness. A TTX, on the other hand, is designed to be a professional tool. Its aim is to test plans, improve coordination, and train participants in handling real-world scenarios, such as cybersecurity incidents or disaster response. This functional purpose often creates a more rigid, goal-oriented environment, where participants feel the pressure of showcasing their expertise to prove they are capable of their duties whatever happens. Due to this, for many participants, a TTX may just feel like another task on their to-do list, rather than an opportunity for reflection and personal or professional growth. Unlike an RPG, where the stakes are fictional, a TTX may feel more intimidating and the overall experience less engaging. In an RPG, the playful environment encourages experimentation. Players make decisions freely, knowing that failure only adds to the drama and enjoyment of the game. A rogue’s failed stealth roll might result in an unexpected combat encounter, but this becomes a fun twist rather than a critical error. In contrast, participants in a TTX may fear making mistakes, especially if the exercise starts feeling like a performance evaluation rather than a learning opportunity. For instance, a junior analyst in a cybersecurity exercise may hesitate to suggest an action that deviates from the standard operating procedure, even if it might work in the scenario and result in a possible improvement in the overall procedure. They might worry that their suggestion will reflect poorly on their competence if it turns out to be wrong in the end or draw criticism from higher-ups for possibly trying to overrule their authority. In fact, this fear can play a significant role in hierarchical organizations with a strict culture where participants are wary of contradicting their superiors. A mid-level manager may hold back an idea during a disaster response exercise because it conflicts with the preferences of a senior executive in the room. Such dynamics not only stifle creativity and engagement but significantly limit the effectiveness of the exercise in the end.

Also, we know that RPGs thrive on voluntary engagement. Players join because they enjoy the process and look forward to creating memorable stories with their peers. In a TTX, participation is often mandatory, and the focus on real-world scenarios can make the experience feel dry or tedious. The participants' mindset is not one of play but of work, and the structured nature of the exercise can feel restrictive rather than empowering. For example, if a TTX is heavily scripted with predetermined outcomes, participants may disengage, seeing little room for their input to matter.

To address these challenges, elements of RPGs' design can be integrated into TTXs to make them more engaging and effective. Borrowing techniques like character roles, branching narratives, and meaningful choices can help bridge the gap, turning "work" into a more immersive and rewarding experience.

For this to happen, the "Facilitator" needs to become a "GM" or, more precisely, the "Cybersecurity Game Master", and the team needs to transform into a "party" where each member has a specific role with unique characteristics and skills.

Let's start with the character classes or, we should say, roles.

The Cybersecurity RPG Classes

We know that the traditional fantasy archetype classes include paladins, rogues, wizards, and so on, but these won't work for us; so we have to replace them with real cybersecurity professional roles and relevant stakeholders, who contribute to managing cyber incidents to reflect the actual expertise within an organization. It is also important to remember that, while each role brings in unique skills and perspectives to the table, not all roles may be required simultaneously in the same exercise as a specific focus (e.g., technical or managerial) may need only the involvement of a certain subgroup of people.

Information Security Analyst (ISA) or Incident Handler (IH)

The ISA acts as the frontline defender of the organization, akin to a possible rogue in an RPG, who scouts an area for possible approaching dangers. These professionals monitor systems, identify potential vulnerabilities, and respond to active threats. In our TTX-RPG, the ISA's key skills revolve around threat detection, vulnerability assessment, and incident response. For instance, the ISA might be able to identify (e.g., by taking into account certain skills and "rolling" a 20-sided die as we will see later) whether an unusual spike in network traffic is a harmless anomaly or the sign of a DDoS attack. Their quick thinking and analytical abilities can often determine whether an incident is mitigated early or spirals into a larger crisis. For simplicity in the context of our simulation, we can assign to this role a broader scope of activities, such as threat analysis, too.

Network Administrator (NetAdmin)

The NetAdmin may be seen as the group's "wizard." They possess a deep understanding of the technical infrastructure and hold the metaphorical "keys" to systems and networks. NetAdmins are crucial for maintaining uptime, securing systems, and managing network configurations. In a TTX scenario, the NetAdmin's tasks might include diagnosing outages, successfully setting up firewalls and modifying their settings on the fly or isolating compromised devices. For example, they could "roll" a d20 to deploy a new firewall rule in time to stop a threat, with a roll higher than a predefined target indicating success without unintended consequences like locking out legitimate users.

Red Teamer (RT) or White Hat Hacker (WHH)

The RT represents the organization's offensive or adversarial mindset, mirroring an RPG's "fighter" class. They simulate attackers, probing for weaknesses in systems, applications, or human behavior. In a TTX-RPG, they might play as an active threat actor (in adversarial scenarios) or as consultants offering insight into potential vulnerabilities.

For example, the RT could roll to exploit vulnerability in a system, with the result determining how effectively they bypass defenses. Their expertise ensures that exercises remain realistic and grounded in potential real-world tactics.

Chief Information Security Officer (CISO)

The CISO is the leader of the cybersecurity response effort, akin to the "paladin" or "commander" archetype. They oversee the organization's strategic defense, ensuring the team's efforts align with business priorities. In a TTX-RPG, the CISO's decisions might focus on resource allocation, communication with executives, and balancing risk against operational needs. For example, the CISO might use their "persuasion" or "communication" skills as a bonus in a roll to gain executive buy-in for isolating a critical server. A high roll reflects successful persuasion, while a low roll could result in pushback from other business units. The CISO's ability to bridge technical and business perspectives is essential in managerial TTX scenarios.

Human Resource Manager (HR Manager)

The HR Manager fulfills a critical, but often overlooked, role that may be compared to that of a team's "cleric" in a traditional RPG. They can be tasked to manage the human side of cybersecurity, handling insider threats, employee compliance, and morale. In a TTX-RPG, the HR Manager might focus on addressing phishing attacks targeting employees or responding to disgruntled insiders.

For instance, they might roll to conduct a damage control meeting after an internal breach. A high roll could calm tensions and ensure compliance, while a low roll could exacerbate the situation and increase the stress level of the participants. The HR Manager's natural focus on human behavior nicely complements the technical roles.

Legal Advisor (LA)

The LA covers a role that can be seen, in RPG terms, kind of similar to the “bard”, that is, someone able to offer support and critical guidance in complex situation that, in this case, could cover aspects such as compliance, liability, and public relations. Their expertise ensures that incident responses adhere to legal and regulatory requirements. In our TTX-RPG, they might roll to evaluate the legal risk of a proposed response strategy or to craft a public-facing statement after a data breach. In this scenario, a high roll would ensure compliance and mitigates fallout, while a low roll might lead to regulatory fines (RF) or RD. This role is particularly vital in exercises involving data breaches or regulatory reporting.

Risk Manager (RM)

The RM is the “strategist” of the group, focusing on identifying and prioritizing risks to the organization. In a TTX-RPG, their role should involve assessing the likelihood and impact of threats, advising on resource allocation, and balancing short-term responses with long-term mitigation strategies. For instance, they could roll to evaluate the potential impact of a ransomware attack, with higher rolls offering more precise and actionable insights. Their ability to quantify risk makes them invaluable for both technical and managerial exercises.

Public Relations (PR) Specialist/Manager

The PRS acts as the organization’s “diplomat”, managing external communication and safeguarding the organization’s reputation during and after a cybersecurity incident. In the context of our TTX-RPG hybrid, this role is critical for exercises that simulate public or media scrutiny, as they craft messages to stakeholders, customers, and the press that can have different repercussions and consequences. For example, the PR Specialist might roll to draft a statement addressing a ransomware attack. A high roll could result in a message that reassures stakeholders while preserving trust, while a low roll might escalate the issue, drawing criticism or panic with the need for further action. The PR Specialist must balance transparency,

accountability, and reputation management, making them essential in high-visibility scenarios.

Forensic Investigator (FI)

The FI takes on the role of a “detective” or, in an adventure-like setup, a “tracker”, diving deep into the technical details to uncover the root cause of incidents and gather evidence for potential legal actions. In the TTX-RPG, their responsibilities can include identifying attack vectors and indications of compromise (IOC), tracing threat actors, and recovering compromised data. For instance, the FI might roll to determine how malware entered the network. A high roll could pinpoint the exact entry point and actor, while a low roll might lead to false assumptions or delayed identification. Their ability to provide actionable insights is essential for technical TTXs and for informing legal or compliance-focused roles.

Now that we know our party of heroes, let’s see how we can bring them to life and characterize them effectively.

Stats and Skills

Like in any RPG, each participant to the game, or, shall we say, exercise, should assume the identity of an alter ego representing a specific role, like those discussed in the previous section, ideally matching their real-life expertise as much as possible. Having an idea of what the character should be doing is not enough though, as everything including every specific action needs to be driven by a set of numbers or, more precisely, by a set of primary stats and derived skills. These need to be general enough to be applicable to all roles but also specific enough to enable for the peculiar characteristics of each particular role to clearly emerge in unique ways. Here, D&Ds define six such stats: Strength, Dexterity, Constitution, Intelligence, Wisdom, and Charisma, which are then used to derive a varied set of skills related to combat, social interactions, and problem-solving like,

for example, agility, knowledge, learning ability, intuition, persuasion, and so on.

Cybersecurity Stats

In our case, the primary stats need to balance simplicity with relevance to real cybersecurity scenarios, so they must capture both technical expertise and soft skills.

For example, we can build our system on the following traits.

Technical Acumen (TA)

TA represents a character's depth of technical knowledge and problem-solving ability in cybersecurity and IT-related matters. This stat underpins roles like the RT, FI, and NetAdmin. High TA enables swift identification of vulnerabilities, efficient debugging, and the ability to deploy technical countermeasures effectively. A character with a high TA could succeed in activities that require to:

- Analyze logs to detect suspicious patterns (e.g., brute-force attacks).
- Dissect malware or reverse-engineer software.
- Deploy intricate firewall rules or network segmentation under pressure.

On the other hand, roles with low TA, such as PR Specialists or HR Managers, might struggle with basic IT-related tasks, needing assistance from more technical teammates.

Strategic Thinking (ST)

ST measures a character's ability to make long-term decisions, prioritize actions, and assess risks. This stat is central to roles like the CISO, RM, and Business Continuity Planner. A high ST allows characters to:

- Effectively allocate resources during a prolonged incident.

- Anticipate threat actor behavior and proactively prepare defenses.
- Manage competing priorities in high-pressure scenarios.

Low ST might manifest as poor decision-making under stress, failing to allocate resources effectively or failure to foresee secondary impacts of decisions.

Communication (COM)

COM measures a character's ability to convey information clearly, persuade others, and manage interpersonal dynamics. It reflects the soft skills needed for collaboration, leadership, and stakeholder engagement. Roles like the PR Specialist, HR Manager, and Legal Counsel need high COM scores more than any others. High COM helps characters:

- Craft effective messaging to external audiences during a crisis, possibly avoiding public backlash or gaining extra time.
- Navigate office politics, persuade others to collaborate and reduce tensions among stakeholders.

Conversely, low COM might hinder collaboration, misrepresent critical details, alienate key team members, or draft a PR message that will make the stock price collapse abruptly.

Analytical Thinking (AN)

AN reflects a character's ability to process information logically, recognize patterns, and solve complex problems. While somewhat similar to Strategic Thinking, AN is more technical in nature and focuses more on processing detailed data and crafting immediate solutions rather than long-term planning. Roles like the FI, ISA, and RT benefit the most from high AN score as it makes easier for characters to:

- Solve puzzles (e.g., decrypting an encrypted file or identifying rogue processes).

- Analyze a flood of alerts to identify the critical incident.
- Connect seemingly unrelated data points to form a coherent picture and get valuable insight.

Low AN could result in tunnel vision, missed opportunities, or errors in analysis.

Leadership (LDR)

LDR represents the ability to inspire, coordinate, and guide a team through crises. It is essential for roles like the CISO and RM, but it can also enhance the contributions of non-leadership roles by encouraging teamwork and boosting morale. High LDR allows characters to:

- Rally the team during chaotic moments, improving overall performance (a boost in morale may give an extra bonus to certain actions and motivate the team to work harder or overtime).
- Provide clear direction and ensure that tasks are prioritized appropriately.
- Negotiate compromises between conflicting priorities.

On the other hand, low LDR could lead to team disarray, indecision, or ineffective conflict resolution.

Resilience (RES)

RES measures a character’s ability to withstand stress, manage pressure, and bounce back from setbacks. RES is vital for all roles, as it determines how well a character maintains their composure and effectiveness during the extended or high-intensity incidents. High RES helps the characters to:

- Stay calm and rational when a plan fails or unexpected challenges arise.
- Recover quickly from failed attempts, adapting to the situation.

- Simulate the ability of the character to maintain focus and energy during prolonged period of stress. Prolonged scenarios may inflict a penalty on certain actions unless a certain resilience score is met.

Low RES may lead to emotional responses, decision paralysis, or burnout during a critical moment.

These six stats can form the backbone of our TTX-RPG system and provide a framework for crafting well-rounded characters. Depending on the role, certain stats will naturally be more critical than others: TA, for example, is essential for technical roles like RT and NetAdmin, while ST and LDR would be more relevant for management roles like the RM or CISO.

In the character creation phase, players would roll 4D6 (four six-sided dice), discard the lowest die, and then sum the remaining three to generate a value for each stat. By following this approach, we would have values ranging from 3 to 18 to naturally fit the standard 20-point scale typical of RPGs. Low rolls are still possible, though, and while this should not be a big problem in general, we do not want specific roles to run the risk of being penalized exactly in their areas of expertise because of an unlucky roll at the beginning of the game exercise. For this reason, it is recommended that each role should have a "core stat" with a minimum value of ten even if the corresponding roll was just a very low number (Table 4.2).

Stats, which sometimes are also called "attributes" in RPG jargon, are the starting point for defining an additional range of skills that the GM will use to help the team in progressing through all the challenges that make up the scenario under discussion. In other words, derived skills represent the practical applications of primary stats. Like for the RPG counterpart, these skills will determine how easy it is for different characters to perform specific tasks within the training exercise or, in other words, their probability to succeed.

To avoid overwhelming players, though, we need to limit the overall number of different skills as much as possible: the skill system needs to be

concise yet comprehensive, with each skill tied to one or more primary stats and influenced by the character's role so that different roles are naturally better at certain activities.

Table 4.2 Core stats for each role ⏎

ROLE	CORE STAT (MINIMUM VALUE = 10)
Information Security Analyst (ISA)	Analytical Thinking (AN)
Network Administrator (NetAdmin)	Technical Acumen (TA)
Red Teamer (RT)	Technical Acumen (TA)
CISO	Leadership (LDR)
HR Manager	Resilience (RES)
Legal Advisor (LA)	Communication (COM)
Risk Manager (RM)	Strategic Thinking (ST)
Public Relation (PR) Specialist	Communication (COM)
Forensic Investigator (FI)	Analytical Thinking (AT)

From a practical perspective, here, each skill should be calculated by combining the bonuses of two relevant stats plus any other relevant bonus, including the character level, as shown in the following formula:

Base Skill Score = Stat 1 Bonus + Stat 2 Bonus + Role Bonus + Level

Where **Stat Bonuses** are calculated based on the primary stat's final value rolled during the character creation phase: for each primary stat, we roll four six-sided dice (4D6), discarding the lowest number and adding the others. Then, we compute the bonus by using the following formula:

Bonus = (Stat value – 10)/2 (rounded to the lowest integer)

In other words, we add 1 for each 2 points above 10, and deduct 1 for every two points below 10 (Table 4.3).

Once again, role bonuses are important to emphasize how certain skills are more relevant to specific roles. Hence, we provide an additional +1 or +2 for skills directly related to a role's expertise. We also want to have an overall sense of progress as characters become more experienced across different exercises so each role should also have a "level" associated to it, starting from one and increasing as XPs are gained by progressing across different challenges, as we will see later.

Table 4.3 Do note how "bonuses" could actually be negative to discourage people to take actions in fields out of their expertise. Indeed, in real life, allowing a penetration tester to write a PR statement or a LA to check some TCP packets transmitted over the network would likely be a recipe for a quick disaster! ⏎

CHARACTER ROLL (4D6, DEDUCT LOWEST DIE AND ADD THE REST)	STAT BONUS
3 or 4	-3
5 or 6	-2
7 or 8	-1
9 to 11	0
12 or 13	+1
14 or 15	+2
16 or 17	+3
18	+4

Cybersecurity Skills

Back to our system, we will use the following skills derived by their associated primary stat bonuses:

1. Incident Response (Based on TA + RES Bonuses)

Incident Response measures the character's ability to react swiftly and effectively to a cybersecurity incident, whether it's isolating infected systems, responding to phishing attacks, or triaging alerts.

Rationale behind stats influence: High TA contributes to technical expertise and high RES ensures calmness and rational thinking under pressure.

Role bonuses:

- RTs get an additional + 2 bonus.
- ISA and NetAdmins get an additional +1 bonus.

Example of possible applications of this skill during an exercise:

- Isolate affected systems during a ransomware attack.
- Identify and neutralize threats in real time.
- Guide the team through immediate response tasks.

2. Forensic Analysis (TA + AN)

Forensic Analysis reflects a character's ability to collect, analyze, and interpret digital evidence. This skill is essential in post-incident investigations or threat attribution.

Rationale behind stats influence: High TA ensures deep technical knowledge. AN supports logical deductions.

Role bonuses:

- FIs get +2.
- ISAs get +1.

Example of possible applications of this skill during an exercise:

- Extract artifacts from memory dumps or hard drives.
- Trace the origin of a malware payload.
- Compile evidence into reports for legal or managerial review.

3. Risk Assessment (ST + AN)

Risk Assessment evaluates a character's ability to identify vulnerabilities, evaluate potential impacts, and prioritize risks.

Rationale behind stats influence: ST provides the foresight needed to assess long-term impacts, while AN helps process complex data.

Role bonuses:

- RMs get +2.
- CISOs get +1.

Example of possible applications of this skill during an exercise:

- Analyze a company's cybersecurity posture.
- Prioritize mitigation strategies based on risk impact.
- Propose resource allocations for maximum effectiveness.

4. Stakeholder Engagement (COM + LDR)

Stakeholder Engagement reflects the ability to communicate effectively with executives, external partners, and other stakeholders. This skill is critical for roles that bridge technical and non-technical domains.

Rationale behind stats influence: High COM facilitates clarity and persuasion, while LDR ensures confidence and authority.

Role bonuses:

- PR Specialists and CISOs get +2.
- LAs and HR Managers gain a +1.

Example of possible applications of this skill during an exercise:

- Explain a breach’s impact to a board of directors.
- Manage external communications during a crisis.
- Negotiate with third-party vendors or regulators.

5. Threat Analysis (AN + TA)

Threat Analysis measures the character’s ability to analyze adversarial tactics, predict attacks, and adapt defensive strategies.

Rationale behind stats influence: AN supports data correlation. TA allows understanding of attack methodologies.

Role bonuses:

- RTs get +2.
- NetAdmins, ISAs, FIs get +1.

Example of possible applications of this skill during an exercise:

- Correlate IoC across multiple sources.
- Predict the next steps of a persistent threat actor.
- Suggest defensive measures based on the latest intelligence.

6. Systems Configuration (TA + ST)

System Configuration reflects a character’s ability to set up, optimize, and secure systems. This skill is crucial for technical roles responsible for infrastructure.

Rationale behind stats influence: TA ensures deep knowledge of systems, while ST supports prioritization of configuration tasks.

Role bonuses:

- NetAdmins get +2.
- ISAs, RTs, FIs get +1.

Example of possible applications of this skill during an exercise:

- Harden servers against known vulnerabilities.
- Configure firewalls, IDS, and backups.
- Respond to misconfigurations under time pressure.

7. Stress Management (RES + COM)

Stress Management measures a character's ability to maintain composure, boost team morale, and navigate tense situations.

Rationale behind stats influence: RES prevents breakdowns under pressure, while COM aids in providing reassurance and focus.

Role bonuses:

- HR Managers and PR Managers get +2.
- LAs and CISOs get +1.

Example of possible applications of this skill during an exercise

- Calm down the team in a critical situation.
- Encourage collaboration despite high-stress conditions.

8. Policy Compliance (ST + COM)

Policy Compliance reflects the ability to interpret and implement organizational policies and ensure adherence to regulations.

Rationale behind stats influence: ST helps align actions with organizational objectives and COM ensures clarity in policy dissemination.

Role bonuses:

- LAs and RMs get +2.
- CISOs and HR Managers get +1.

Example of possible applications of this skill during an exercise:

- Interpret and correctly follow legal and regulatory requirements.
- Align incident response actions with organizational policies.

Table 4.4 offers a summary of skills available in the system.

Applying the System

As an example, let's imagine we are the FI in our team, and we are getting ready to participate in a gamified TTX. The first step would be to prepare our alter ego to cover such a role. We can name him Dr. Robot and then proceed by rolling all the necessary stats and skills. These should get neatly summarized into a character sheet to keep track of our progress (see Appendix C for the character sheet template).

Table 4.4 Summary of skills. Note that not all skills and roles may be relevant within a single exercise. ⏎

SKILL	STAT 1	STAT 2	+2 ROLE BONUS TO	+1 ROLE BONUS TO
Incident Response	TA	RES	RT	ISA, NetAdmin
Forensic Analysis	TA	AN	FI	ISA
Risk Assessment	ST	AN	RM	CISO
Stakeholder Engagement	COM	LDR	CISO, PR	LA, HR
Threat Analysis	TA	AN	RT	NetAdmin, ISA, FI
Systems Configuration	TA	ST	NetAdmin	RT, FI, ISA

SKILL	STAT 1	STAT 2	+2 ROLE BONUS TO	+1 ROLE BONUS TO
Stress Management	RES	COM	HR, PR	LA, CISO
Policy Compliance	ST	COM	LA, RM	CISO, HR

Dr. Robot starts as a Level 1 character with zero experience. Our first 4D6 roll is for TA, which is also our core skill so we will reject a score less than 10, is 6,4,1,3. We discard the lowest die, 1 in this case, and we get a 13, giving us also a +1 bonus modifier. For ST, we roll 4,5,3,1, giving us 12 + 1 bonus, and we proceed like this to complete all our primary stats. Once done, we can combine our results to derive all the skills (do not forget that FIs receive a +2 skill bonus in Forensic Analysis and +1 bonus in Threat Analysis as per Table 4.4!) and complete our character sheet:

Character Sheet

Name: Dr. Robot **Role:** FI **Level:** 1 **XP:** 0/10

XP System: XP is awarded for passing challenges according to the formula: DC/10, rounded to the nearest integer. Level Progression: XP required to level up = 10 × Current Level

As we see, in this case we rolled out quite a skilled character: Dr. Robot is not only proficient in the technical areas required by his job function, but he is also gifted with communication skills that can potentially enable him to interact directly with stakeholders if needed. On the other hand, his low resilience score may influence the outcome of certain actions if the scenario under analysis puts him under some high stress situation. Throughout the exercise, in fact, the GM who, from now on, we should start calling as the “Cybersecurity Game Master” or CGM, will lead the narrative-based exercise and pose a constant barrage of probing questions and situations for the characters to solve. These challenges should be related to the previous skills and, like for the RPG counterparts, identified by the “Difficulty Challenge” (sometimes also referred to as “Difficulty Class” or, more simply, DC). This represents a target value that players need to match or

beat by rolling a “skill check”. Skill checks are central to the TTX-RPG system, as they determine the success or failure of actions based on character stats, derived skills, and the difficulty of the task. In general, a skill check involves:

Table 4.5 Primary stats (Base: 4D6, drop lowest. Max 18, Min 3 before bonuses)

STAT	ABBREVIATION	VALUE	MOD (FLOOR((VALUE-10)/2))
Technical Acumen	TA	13	1
Strategic Thinking	ST	12	1
Analytical Thinking	AN	14	2
Resilience	RES	6	-2
Communication	COM	16	3
Leadership	LDR	12	1

Modifiers: For every 2 points above 10, add +1 to relevant skills. For every 2 points below 10, deduct 1 instead.

Table 4.6 Derived skills (Base = Sum of relevant stat modifiers + role bonuses + Level)

SKILL	RELEVANT STATS BONUSES	ROLE BONUS	LEVEL	TOTAL
Threat Analysis	AN + TA: 3	1	1	5
Incident Response	TA + RES: -1	-	1	0
Forensic Analysis	TA + AN: 3	2	1	6
System Configuration	TA + ST: 2	-	1	3
Policy Compliance	ST + COM: 4	-	1	5

SKILL	RELEVANT STATS BONUSES	ROLE BONUS	LEVEL	TOTAL
Risk Assessment	ST + AN: 3	-	1	4
Stakeholder Engagement	COM + LDR: 4	-	1	5
Stress Management	RES + COM: 1	-	1	2

- Rolling a 20-sided die (D20).
- Adding the relevant skill scores (derived from primary stats and/or role bonuses as instructed by the narrative of the exercise).
- Comparing the total to a predefined DC target value, set in accordance with the perceived difficulty (see Table 4.7).
- If the total is equal or greater than the target, the action is successful and, in our system, the player gets XPs equal to DC/10, rounded to the nearest integer. Either way, the narrative continues accordingly.

To better understand how all this works in practice, let's imagine a simple TTX data breach scenario and focus on the role of our imaginary friend, Dr. Robot:

RPG-TTX Example: Data Breach

On the morning of February 16, the Security Operations Center (SOC) at Evil Onion Corp. detected anomalous outbound network traffic from a critical database server. The traffic, flagged by a Data Loss Prevention tool, indicated large amounts of customer financial records being transmitted to an external IP address linked to a known threat actor group. Internal logs suggest unauthorized access through a compromised VPN credential.

The organization's CISO has tasked the FI with conducting a detailed analysis to determine how the breach occurred, identify the scope of the compromise, and provide recommendations to prevent future incidents.

Table 4.7 Typical target values for Difficulty Challenges. Of course, anything in between is also possible. Note how Hard and Extreme require significant bonuses (or players having already acquired advanced levels of experience) besides a good roll of the D20. ⏎

DIFFICULTY CHALLENGES LEVEL	TARGET VALUE (ROLL A NUMBER EQUAL TO OR GREATER THAN TO BEAT IT)
Easy	10
Moderate	15
Hard	20
Extreme	25

The narrative should reference, and let the players getting familiar with, the following MITRE ATT&CK TTPs:

- Valid Accounts (T1078.004): The attackers leveraged stolen VPN credentials to gain access to the network.
- Command and Scripting Interpreter (T1059.001): Evidence of PowerShell scripts executing malicious commands was found in system logs.
- Credential Dumping (T1003.001): Attackers used Mimikatz to extract additional credentials from memory.
- Exfiltration Over C2 Channel (T1041): The attackers used an encrypted channel to exfiltrate data to an external server.

During the exercise, the FI should take the lead to analyze network logs, review endpoint artifacts, and correlate findings to establish the full attack chain.

After the CGM has introduced the scenario, the team should be asked how they intend to proceed. Any player with an AN or LDR stat base value equal to or greater than 12 should be allowed to answer this, likely by saying something along the lines of

According to our IRP, we should work to identify how the attacker gained access.

The ball then rolls to our FI who is tasked with the examination of VPN access logs and cross-references them with known compromised credentials from an earlier phishing campaign. This first part can also be role-played with a DC = 12 by considering the Policy Compliance skill bonus (+5 for Dr. Robot), in case the character does not take such initiative himself. If the D20 roll is at least a 7, we match the DC and Dr. Robot gets the logs plus 1 XP point (1.2 rounded), which he should also get if he proactively requested the logs to the CGM without being explicitly prompted to do so. On the other hand, if the roll fails, Dr. Robot would get a –1 to his Policy Compliance skill for the rest of the exercise.

One way or the other, Dr. Robot will get the logs in the end and be informed he now needs to go through them to look for cues to continue the exercise.

Whether Dr. Robot finds anything useful in the logs, though, is not guaranteed. It is determined by his skill in Threat Analysis (AN + TA) and whether he is able to pass a corresponding challenge with DC = 10 or not.

If the skill roll succeeds, the investigator is informed by the CGM that he successfully identified unauthorized logins from an unusual geolocation outside normal operating hours, allowing the NetAdmin to step in, block further access, and revoke compromised credentials. If the roll fails, instead he would be unable to pinpoint the source of access, leading to delays in containment. If this happens, anybody with Resilience less than 14 will get a -1 to their Stress Management bonus for the rest of the TTX.

Dr. Robot would, then be allowed to try again with a reduced DC (3 points less for each additional attempt, e.g., to be decided by the CGM if not explicitly discussed in the exercise plan) but, in the meantime, the CGM can assume that the attacker has retained network access for an extended period of time, escalating the threat and provoking additional financial damage to be evaluated later by the legal team.

With this first challenge behind, the CGM continues the narrative by asking the team what their next steps would be according to the relevant playbook. For example, the FI may now be asked to determine if additional credentials were compromised. To do so, Dr. Robot now decides to examine memory dumps from affected servers for traces of credential dumping tools like Mimikatz. From our RPG perspective, now we have a “Memory Analysis for Credential Dumping” challenge with DC = 15 with Forensic Analysis (TA + AN) as the relevant skill to look at.

If the check is successful, the investigator finds evidence of Mimikatz execution and recovers a list of stolen credentials. The NetAdmin can then proceed to execute the needed password resets and privilege revocation, in time for preventing further lateral movement.

On the other hand, if the check fails, it means the investigator overlooked critical artifacts, allowing the attacker to use stolen credentials for deeper network penetration, hence, opening up the possibility of narrative injects requesting the intervention of other team members to support the investigation. Once again, in case of failure, the team should be ready to face increased pressure, here represented by an additional penalty in Stress Management. The PR Manager may also have to craft a letter to stakeholders to justify the delays (will the stakeholders be satisfied? Like every other action, this will have to be role-played by the relevant team member with an appropriate DC), before the FI can have a second look with an easier DC to uncover the origin of the breach.

As the incident progresses towards a conclusion, the FI must then determine how the data was exfiltrated and whether any information remains at risk. By reviewing firewall logs, proxy logs, and endpoint telemetry, Dr. Robot can attempt to identify the exfiltration channel. Again, this may be the recommended step in the playbook or be recommended by the CGM if no one in team knows how to proceed. In this case, the relevant skill would be “Incident Response” (TA + RES) and we have a DC = 15.

If the skill roll is successful, Dr. Robot is informed that he identified the attacker’s command-and-control (C2) infrastructure, and he is able to block further communication. If the roll fails, instead, it would mean that he

misidentified the exfiltration channel, missing an alternate route for the attackers to successfully extract additional sensitive data before containment measures take effect.

In the end, if the technical team successfully uncovered all major attack vectors quickly, Evil Onion Corp. should be able to rapidly contain the incident, preventing further data loss. However, failures at any stage increase the complexity of response efforts, allowing the attacker more time to pivot and exfiltrate additional information, the consequences of which should be evaluated, as part of the exercise, by the management and/or legal teams, adding additional learning opportunities to the overall exercise.

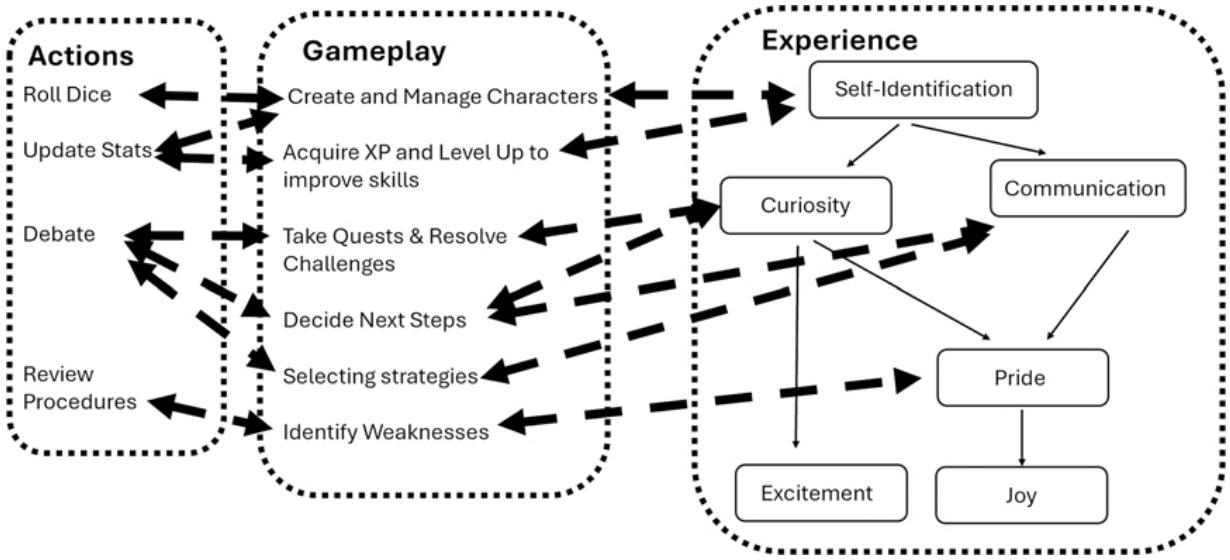

Figure 4.2 AGE analysis for the gamified RPG-TTX discussed in this chapter. Adding the RPG elements to the mix helps delivering a much more engaging exercise where team members can delegate their successes as well as their failures to overcome specific challenges to their alter ego character, increasing self-identification and overall excitement compared to standard TTX exercises. ⏎

Practicing this scenario in a TTX would allow the team to train and get a better comprehension of all the relevant procedures involved. At the same time, adding the RPG elements allows for an even more engaging experience (see Figure 4.2), where failing at specific tasks gives an

opportunity for further exploration and additional learning opportunities while also avoiding direct blame on a specific person (“*hey! I just got a bad D20 roll, it’s not my fault, I know what to do, it was just bad luck!”*).

5
Making the Most out of an RPG-TTX

DOI: 10.1201/9781003606314-6

In Chapter 3, we discussed some basic principles of RPG quest design while, in Chapter 4, we had a first RPG-TTX example following the definition of our gamified systems. Now let's explore how to adapt those principles within a professional cybersecurity context, assuming we have the IRP and Playbooks as foundational resources.

Creating Relevant and Engaging Cybersecurity Quests

There are several ways a CGM can start planning for an engaging RPG-TTX quest. For example, we know the IRP provides a high-level framework for responding to incidents, making it an ideal starting point for quest design. Each typical section of the IRP, that is, Preparation, Detection, Containment, Eradication, and Recovery, can serve as the foundation for a quest, depending of which specific area the TTX is supposed to look into. We could have a "Preparation Quest" where players must review, and eventually update, the IRP based on a new threat landscape, such as the rise of AI-powered phishing attacks: how would the team react? Does the specific incident fall into an existing category and is properly covered? Are all the roles clear in that case? On the other hand, a more technical quest may instead focus on the detection part of the IRP, where players are tasked with identifying a potential breach after receiving an alert about unusual

login activity, and then move to check the effectiveness of the most appropriate playbook available.

Playbooks, in fact, are among the most important guides that need to be tested and, eventually, updated. Let’s not forget that, while the IRP provides the framework, the Playbooks give us the actual practical details we can use and reference into a quest. Since each Playbook corresponds to a type of incident, for example, ransomware, DDoS attacks, or insider threats, these are natural starting points to design quests that mirror real-world scenarios.

A Ransomware Quest may force the team to face a scenario where a ransomware attack that has encrypted critical systems. By looking at what is included in the playbook, the CGM could include sections on negotiating with attackers, restoring data from backups, and communicating with all the relevant stakeholders. Will the team member implement the instructions properly? And, most importantly, would any question be raised on the effectiveness of the playbook while “playing” through it to further improve it?

In any case, no matter what the specific topic is, a good quest must have some branching narrative and be able to cover potentially unexpected situations. We know that one of the most powerful aspects of RPGs is the ability to adapt based on player choices. In a cybersecurity quest, we can try to achieve this by matching critical situations to possible branching outcomes of skill checks, like we saw in the Chapter 4 example. These should not only affect the stats of the players but also impact the ongoing scenario in ways that are still meaningful and worth exploring. For example, if an RM fails a skill check while assessing the impact of a breach, the narrative could branch to include RFs or public backlash that the team now has to deal with accordingly. Or an RT may decide to investigate a certain configuration that, if successful, might expose a right away new, previously undetected threat, saving the team much more trouble at a later time.

These branches not only make the quest more dynamic but also provide opportunities for additional discussions and learning. When players fail a skill check, it should not be a moment of disappointment or shame but a

teachable moment, making the team curious about possible consequences to highlight areas for improvement in a potentially critical situation.

The current documentation should not serve as the only source of inspiration to design the upcoming challenges, though. To make quests feel even more authentic, we should also look at real-world incidents. And, unfortunately, we have no shortage of such incidents around us: what could our team do in a situation similar to the SolarWinds Supply Chain Attack [1], for example? Here we could design a quest where the team must investigate a compromised software update, trace the attack's origin, and mitigate its impact. Or we could look at the Equifax Data Breach case [2] and create a quest focused on identifying and patching vulnerability in a web application before attackers can exploit it. By grounding quests in real-world events, we not only make them more engaging but also ensure that the team is learning skills that are directly applicable to their roles in a real crisis.

Another important feature of good quest design is the ability to keep players on their toes, so to speak, so that they do not relax once things seem under control. "Inject" as sudden, unexpected events, are a great resource for this purpose and a powerful tool for maintaining engagement by simulating the unpredictability of real-world incidents. Injects should feel organic to the situation under analysis, though, and have to seamlessly integrate into the narrative. They should never feel like arbitrary disruptions. Luckily, we can easily justify these by tying them to failed skill checks or at key moments to escalate the scenario in some meaningful way. For example, if the FI fails to analyze a malware sample, the CGM can introduce an inject about the malware spreading to additional systems producing additional, unexpected problems. Or, if the CISO fails a communication check, we can introduce an inject about a negative news article going viral and causing unexpected consequences for the management team to prioritize and address right away.

To illustrate these ideas in action, let's walk through the main points of a possible quest inspired by the Colonial Pipeline ransomware attack [3].

Objective: Contain and mitigate a ransomware attack that has encrypted critical systems.

Setup: An unknown APT group has successfully breached the network and deployed ransomware. The team must respond before it's too late.

Core Narrative points across the main phases of the incident may include:

Detection: The team receives an alert about unusual activity on the network. If the Security Analyst succeeds in a detection skill check, they identify the ransomware early. If they fail, the alert is classified as a false positive and the ransomware spreads to additional systems.

Containment: The team must isolate all the infected systems. If the NetAdmin fails a containment skill check, the ransomware spreads further, requiring additional resources to mitigate.

Eradication: The team must remove the ransomware and restore systems from backups. If the FI fails an analysis skill check, they miss a critical detail, leading to a reinfection.

Recovery: The team must communicate with stakeholders and ensure systems are fully restored. If the CISO or the PR lead fails a communication skill check, the organization may still face RD, and an additional scenario may open up.

Possible Injects:

- Backups for data recovery got corrupted! The probability of this happening should be dependent on how they are managed and handled.
- A news article about the attack goes viral due to an unknown whistleblower, forcing the team to address public relations in more detail.
- The attackers demand a higher ransom or threaten to release some very sensitive company information, escalating the pressure on the team and possibly encouraging them to reconsider a previous decision (e.g., paying the ransom).

How to Debrief Players

Before diving head-on into a cybersecurity RPG-TTX exercise, it is also important to set the stage properly. Players should not feel like they are simply walking into another routine meeting or training session but, like for an actual RPG, they should be immersed in the experience from the beginning. The CGM is also responsible for crafting this welcoming and engaging environment, ensuring that participants understand the purpose of the session, their roles within it, and the mechanics that will guide their decision-making.

To begin, the CGM should introduce the scenario in a way that captures attention. Instead of simply stating, “Today, we will be running an incident response tabletop exercise”, they should open with a more engaging hook:

> *The SOC receives an alert as some unusual outbound traffic from an internal file server is detected. Initial analysis suggests data exfiltration. The company’s board has been informed, and executive leadership is demanding immediate answers. Your team has been assembled to assess the situation, mitigate the damage, and ensure this does not happen again. Time is of the essence. Are you ready?*

This narrative framing immediately signals to participants that they are stepping into a simulated crisis, where urgent action is required, and their decisions will have meaningful consequences. Then, if not already done beforehand, the CGM introduces the relevant rules, explaining the character roles, stats, and skill checks that will determine success or failure in various challenges. Rather than overwhelming players with excessive rules, the explanation should be light and engaging, emphasizing that this is a guided, but flexible, exercise and he will do anything so that they can freely decide the course of action they believe is the best. At this stage, if needed, the CGM should also help the participants in the creation process of their own alter ego characters, who will be covering their roles in the simulated scenario.

Once the game is underway, the CGM carefully follows and moderates the flow of the session. The objective is to maintain engagement, keeping

players focused on informed decision-making while ensuring that the scenario remains plausible and relevant. When players attempt a specific action, for example, analyzing logs, using some tool to contain an incident, or briefing executives, a skill check determines whether they succeed or fail, leading to different branching consequences like in the examples illustrated previously.

For instance, if an FI attempts a Threat Analysis check to understand the attacker's techniques but rolls poorly and fails, the CGM might say:

> *Your analysis is inconclusive. The data appears fragmented, and while you have some indicators of compromise, you cannot confidently map them to a known attack pattern. This delay means the adversary may still be inside your network. What do you do next?*

Do note that a failure should never mean that the scenario halts. Instead, it should introduce complications that force further problem-solving. Conversely, a success might reveal the attacker's TTPs as mapped to the MITRE ATT&CK framework, giving the team a clear direction for containment. Also, do keep in mind that, throughout the exercise, injects can, and should, be used to keep players on their toes. A sudden board inquiry demanding an immediate report, a journalist emailing the press office for comment, or a secondary breach escalating the situation, can, for example, add exciting challenges, ensuring that the session remains dynamic and engaging throughout. While the original quest script may try to be as comprehensive as possible, the CGM will always have to adapt and improvise based on the requests, thoughts, and actions from the team.

Once the exercise reaches its resolution, whether through containment, a simulated regulatory fallout, or ongoing mitigation efforts, the transition to debriefing is also critical. Here, it is not recommended that the team is immediately thrust back into a traditional meeting format but, instead, the CGM should maintain the immersive tone, framing the debrief as a reflection on the quest they just played through.

A productive debrief begins by revisiting key moments of the exercise. The CGM might highlight decisions that significantly impacted the outcome, asking open-ended questions to encourage discussion. For example:

> *When you chose to focus on isolating the compromised server rather than tracing the attacker's lateral movement, what was your reasoning? In hindsight, would you have done anything differently?*

Rather than simply pointing out failures, the discussion should explore the rationale behind decisions. Players should feel comfortable acknowledging mistakes, which require a debriefing environment where there is no fear of judgment. The CGM can facilitate this by acknowledging that real-world incident response is fraught with uncertainty and that even seasoned professionals sometimes make suboptimal choices under pressure, besides there is always the chance of an unlucky roll!

Another useful approach is to connect the in-game actions to actual cybersecurity principles and frameworks. If the team struggled with containment and did not know what to do, for instance, this may imply that the incident playbooks may not be very clear or miss important details and need to be revised. The CGM might reference best practices from NIST or ISO guidelines, bridging the gap between the exercise and real-world applications. Similarly, mapping the attacker's actions to MITRE ATT&CK tactics can reinforce the importance of threat intelligence in shaping incident response strategies.

Finally, the CGM should always try to end the session by providing some actionable takeaways. Rather than a generic summary, the CGM should work with the team to identify specific improvements that can be applied in real life. If communication bottlenecks were an issue, this might lead to a review of escalation procedures. If forensic analysis proved difficult, it could prompt additional training in digital evidence collection. The success of an RPG-TTX exercise does not rest solely on how well the team "performed" during the session, but on whether they leave with a deeper

understanding of cybersecurity challenges and a commitment to improving their real-world readiness. All this can only be achieved if the players are engaged in every single phase of the process and then look forward to the next quest-based training. Remember: the main key drivers of successful gamification are the internal motivators!

How to Measure Success: A Cybersecurity Game Master's Perspective

After the immersive experience of an RPG-TTX session, it is essential to determine whether the exercise was successful and achieved its intended goals. Unlike traditional TTXs, which might be assessed through simple checklists and basic procedural reviews, the RPG-TTX format allows for a more nuanced retrospective. The beauty of an RPG-TTX, in fact, is not just that it gives us an opportunity to verify whether participants can follow the protocols properly, but, most importantly, it provides us with unique insights on the decision-making processes, team dynamics, and problem-solving approaches at a deeper level. Here, the team is constantly prompted with unexpected situations. The uncertain outcomes of skill checks throughout the scenario means they may not always be able to achieve what they desire since something may go wrong unexpectedly and at the worst possible moment, like in real life.

When evaluating a team's performance across the scenario, the CGM should focus on three key dimensions: player engagement and immersion, team performance and decision-making, and real-world applicability. Let's check these one by one.

Assessing Players' Engagement and Immersion

As we have discussed at length, one of the core strengths of an RPG-TTX is its ability to create an engaging and dynamic experience. However, engagement is not just about enjoyment, but it must also directly affect learning outcomes. If participants were actively involved, made thoughtful

decisions, and immersed themselves in their roles, the exercise likely had a meaningful impact. The CGM can gauge engagement through post-exercise surveys and direct observations. Did players stay in character? Were they proactive in their roles? Did they collaborate effectively, or did they disengage? A simple post-exercise self-assessment can help capture these insights, with players rating their immersion, comfort in decision-making, and sense of agency within the scenario. Collecting meaningful and explicit feedback is always an essential step in any activity.

Additionally, more implicit cues can also be used: observing body language and participation levels during the session provides valuable data, too. If certain roles remained silent or if discussions were dominated by a few individuals, this could indicate barriers to engagement. In such cases, some adjustments, such as redesigning role responsibilities or introducing more structured turn-based interactions, might be necessary in future sessions.

Evaluating Team Performance and Decision-Making

The heart of any TTX lies in how teams approach problem-solving under pressure. In an RPG-TTX, we know that decision-making is influenced by both individual skill rolls and collective strategy. Hence, a well-structured retrospective should examine not only the outcomes of each decision but also the processes behind them to identify whether the right procedures were followed and all the available information used effectively.

One effective way to analyze decision-making is through a timeline reconstruction of key events. The CGM, having at hand a “log” of the session, can review how the team responded to various injects and challenge by focusing on the following questions:

- What decisions were made at critical junctures?
- How did players justify their choices?
- Were decisions based on structured reasoning, brainstorming, deference to hierarchy, or even just panic?

- Did the group easily adapt when new information emerged or did they find it difficult to alter the course of their thinking?

A retrospective discussion should avoid labeling decisions as simply “right” or “wrong” but instead focus on what participants learned from their choices. To reiterate, the point of a failed skill check or an incorrect assumption is to lead to a productive discussion on how to refine response strategies.

Additionally, the CGM can also assess how well participants leveraged their character roles. If technical specialists like FIs or RTs took the lead in analysis, while leadership-focused roles like the CISO or RM facilitated strategic decision-making, this indicates that players effectively self-identified into their assigned responsibilities. If, however, certain roles were underutilized or sidelined, it may be necessary to revise role definitions to ensure a more balanced experience.

Measuring Real-World Applicability

No matter how fun and engaging the experience is, ultimately, the effectiveness of any form of training should be judged by whether it translates into improved real-world readiness. This means that the exercise should not exist in isolation, but, instead, it should provide actionable insights that influence actual security practices.

To measure real-world applicability, the CGM should double check that the team was not carried away by their mission and all the exercise’s events and decisions were taken by actually following the relevant company policies, IRPs, playbooks, and past security incidents. Were best practices followed? Did players uncover gaps in procedures? Did any critical vulnerabilities or misalignments between policy and execution emerge? These are key questions the CGM needs to address in reviewing the training and the answers can lead to very significant improvements such as policy adjustments (including updates of relevant escalation procedures and documentation), skill development (maybe the team members need additional forensic analysis training workshops or crisis communication

classes?) or different process enhancements to refine coordination between technical teams, legal, and executive leadership during a security incident.

Last, it is important to add that, while much of an RPG-TTX's impact is best assessed through discussion and reflection, some quantitative measures can also provide additional insights and give more food for thoughts on how the team is able to perform under stress.

Possible metrics to look at can include:

- Response Times: how long did it take for the team to identify the breach, implement containment, and coordinate communication?
- Accuracy of Analysis: how close were players' assessments of the incident to the actual attack scenario?
- Role Utilization: how many skill checks were attempted per role? Were certain roles significantly more or less active? If so, was this due to the specific design of the incident or someone tried to shy away?
- Player Feedback Scores: how did participants rate the exercise in terms of engagement, difficulty, and usefulness?

These metrics should not be viewed in isolation but combined with qualitative feedback to provide a holistic picture of the exercise's effectiveness.

References

1. *Solar Winds*: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know ⏎
2. *Equifax Data Breach*: https://www.csoonline.com/article/567833/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html ⏎
3. *Colonial Pipeline Ransomware Attack*: https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack ⏎

6
Intermezzo: Expert Interviews

DOI: 10.1201/9781003606314-7

Ms. Francesca Bosco, CyberPeace Institute

Francesca Bosco is Chief Strategy Officer at the CyberPeace Institute, an international nonprofit working to reduce the harms from cyberattacks on vulnerable communities and under-resourced organizations, and to ensure human rights are respected in cyberspace. The Institute supports humanitarian, development, and nonprofit organizations by providing practical cybersecurity assistance, conducting analysis on cyberattacks and disinformation, exposing cyber harm, and advancing responsible behavior in cyberspace through multi-stakeholder cooperation.

With over 18 years of experience at the intersection of international law, human rights, and cybersecurity, Francesca has held senior roles at the United Nations and the World Economic Forum. Her work focuses on systemic risks and opportunities from emerging technologies such as AI (Artificial Intelligence) and quantum computing, and she has led programs addressing cybercrime, critical infrastructure protection, disinformation, and the misuse of technology. Francesca connects global policy frameworks with operational implementation, ensuring that cybersecurity and cyber capacity building efforts are context-specific, sustainable, and aligned with development priorities. She advises leaders and boards on integrating cybersecurity into governance to foster responsible technology use, leads

initiatives to promote diversity and inclusion in the field, and connects global policy with practical, on-the-ground implementation.

Dear Francesca, as a leader in cybersecurity strategy for nonprofits, how do you see the unique challenges these organizations face compared to corporate or government entities?

Nonprofits face a unique set of challenges when it comes to cybersecurity, largely due to their resource constraints, limited technical expertise, and the often-decentralized nature of their operations. Unlike corporate or government entities, nonprofits typically operate with smaller teams and may not have the budget to invest in the latest security technologies or dedicated cybersecurity staff. This makes them more vulnerable to attacks, as they may lack the necessary defenses to fend off increasingly sophisticated threats.

One of the main challenges is the lack of awareness and training across the nonprofit sector. Many employees and volunteers in nonprofits wear multiple hats, and cybersecurity often becomes an afterthought rather than a priority. This knowledge gap is a significant barrier, as nonprofits must be able to recognize the threats they face, such as phishing attacks, ransomware, and data breaches, and understand how to mitigate those risks effectively.

One of the emerging risks in this landscape is the uptake of emerging technologies, particularly AI, by under-resourced organizations. While many industry leaders and government entities have the resources to invest in cutting-edge technologies and safeguard them with robust security measures, nonprofits often face significant barriers. These include the high cost of AI-powered tools, the complexity of integrating these technologies securely, and the asymmetry in technical capability between nonprofit organizations and larger, well-resourced industry players or government agencies. As nonprofits adopt AI and other advanced technologies, the lack of expertise and investment in cybersecurity can amplify vulnerabilities, putting sensitive data and operations at greater risk.

Additionally, the rapid pace of AI development and its potential for both positive and negative impacts raise further concerns. Nonprofits, particularly those working with vulnerable populations or sensitive data, must carefully navigate this landscape to avoid exacerbating existing cybersecurity risks while trying to leverage these tools for their missions. The adoption of AI without the proper security measures and training could lead to unintended consequences, such as increased exposure to AI-driven cyberattacks, data manipulation, or privacy violations, with far-reaching implications for both the organization's reputation and its mission.

Furthermore, nonprofits, especially those working with sensitive data, face the added complexity of complying with industry-specific regulations, such as Health Insurance Portability and Accountability Act (HIPAA) for healthcare-related nonprofits or General Data Protection Regulation (GDPR) for those operating in Europe. Compliance becomes particularly challenging when resources are limited and cybersecurity is not seen as a key area of investment.

Another key difference is the nonprofit's reliance on partnerships and collaborations. While government and corporate organizations tend to have centralized control over their cybersecurity, nonprofits often rely on external partners, donors, or cloud providers for their IT infrastructure. This decentralized model creates additional layers of complexity and potential vulnerabilities, as nonprofits need to ensure their partners and vendors maintain strong cybersecurity postures.

Finally, the reputation risk is significant in the nonprofit sector. For many nonprofits, their credibility and trustworthiness are tied to their ability to protect donor and beneficiary data. A cybersecurity incident can have far-reaching consequences for a nonprofit's ability to maintain relationships with donors, partners, and beneficiaries, potentially resulting in lost funding and diminished impact.

In response to these challenges, the cybersecurity landscape for nonprofits is evolving. Increasingly, nonprofits are adopting risk-based approaches, which allow them to prioritize cybersecurity efforts based on the resources available and the critical assets that need protection. Training

and awareness initiatives tailored to nonprofit employees and volunteers are also becoming a priority, as is the development of strategic partnerships with other nonprofits and cybersecurity providers that can offer cost-effective solutions. Additionally, there is a growing recognition that cybersecurity isn't just a technical issue but a strategic one that requires involvement from leadership at all levels of the organization.

In summary, nonprofits face unique challenges due to limited resources, the lack of specialized cybersecurity expertise, and the need to balance security with other priorities. However, with the right approach and resources, nonprofits can significantly improve their cybersecurity posture and ensure their ongoing mission of serving their communities is protected from evolving digital threats.

Key Challenges

1. Limited Resources and Technical Expertise Nonprofits often operate on tight budgets, where cybersecurity can be seen as a secondary priority. According to the 2023 CyberPeace Analytical Report – NGOs Serving Humanity at Risk: Cyber Threats Affecting "International Geneva", 41% of NGOs reported having experienced a cyberattack in recent years. Furthermore, 33% of nonprofits lack IT support or dedicated cybersecurity staff, which significantly increases their exposure to cyber risks. This reflects a widespread vulnerability, as many organizations lack the resources needed to implement basic cybersecurity measures such as conducting regular security assessments or keeping systems up to date. Additionally, the uptake of emerging technologies, particularly AI, introduces new risks for under-resourced organizations. While AI has the potential to drive efficiency, many nonprofits struggle to adopt these technologies securely due to a lack of expertise and financial constraints. AI tools may increase vulnerability if not properly secured, especially when nonprofits lack the cybersecurity investments needed to protect sensitive data from AI-driven threats. NetHope's 2024 State of Humanitarian and

Development Cybersecurity Report corroborates this, noting that nonprofits struggle to implement effective cybersecurity due to financial constraints, and as a result, they often fail to deploy proactive measures to safeguard against threats.

2. Lack of Cybersecurity Awareness and Training A significant barrier for nonprofits is the lack of cybersecurity awareness and training for staff. According to CyberPeace Institute, 85% of NGOs acknowledge the importance of cybersecurity, yet only 52% offer regular cybersecurity training. This gap between recognition and action underscores the need for comprehensive training programs that empower staff to recognize and respond to emerging cyber threats. TechSoup's 2022 Cybersecurity Solutions for Nonprofits highlights a critical issue: nonprofits often prioritize operational tasks over cybersecurity education. It stresses that while nonprofits generally understand the need for secure operations, they often fail to invest adequately in building a culture of cyber hygiene, which is crucial in preventing common cyberattacks like phishing and malware.
3. Compliance and Sensitive Data Management Many nonprofits, especially those working with sensitive data (e.g., healthcare or financial information), face significant compliance challenges with regulations such as GDPR. Nonprofits often struggle to allocate sufficient resources to meet these regulatory requirements, leaving them exposed to potential penalties and RD. According to NetHope's 2024 State of Humanitarian and Development Cybersecurity Report, many NGOs, particularly in the humanitarian and development sectors, face difficulties meeting compliance standards due to the limited cybersecurity capacity within their organizations. This challenge is further exacerbated by the lack of dedicated cybersecurity staff, making it difficult for nonprofits to keep pace with evolving data protection laws. Nonprofits need to develop better compliance frameworks and allocate resources for regular audits to ensure they adhere to these regulations.

4. Dependence on Third-Party Vendors and Cloud Services Nonprofits often rely on third-party vendors and cloud service providers for their IT infrastructure, which introduces additional risks. The CyberPeace Institute's 2023 report found that many NGOs struggle to effectively assess and manage third-party risks. These risks arise when external vendors or cloud service providers do not adhere to the same stringent cybersecurity standards as the nonprofit organization itself. This creates vulnerabilities that could allow attackers to exploit weaknesses in a third-party system, potentially compromising the nonprofit's data or operations. The report recommends that nonprofits implement vendor risk management strategies and conduct regular security audits to reduce exposure to third-party vulnerabilities. Without these measures, nonprofits risk exposing themselves to external breaches that could compromise their systems and data.
5. Reputation and Trust Risks Trust and credibility are essential for nonprofits, as they rely heavily on the support of donors, stakeholders, and beneficiaries. A cyberattack or data breach can severely damage an NGO's reputation, resulting in lost funding and a decline in public confidence. The CyberPeace Institute's 2023 report emphasizes that RD is one of the top concerns for nonprofits in the wake of a cyberattack. The fallout from such incidents can have long-lasting effects, not only on their financial stability but also on their ability to maintain essential partnerships and trust within the communities they serve. NetHope's report further supports this by noting that many nonprofits report being more concerned with the RD caused by cyberattacks than with direct financial losses. These losses are often harder to quantify but can significantly impact the long-term viability of the organization, leading to a reduction in donor support and trust.

How do you balance immediate operational cybersecurity needs (e.g., phishing, patch management) with long-term strategic goals (e.g., building cyber resilience, securing donor data) in resource-constrained nonprofits?

It’s all about balancing the urgent with the important. We start by helping NGOs implement low-effort, high-impact measures – like enabling MFA or running basic phishing simulations. But we also encourage organizations to think long-term: to develop IRPs, build internal awareness, and make cybersecurity part of their risk management strategy. Even small steps can lead to significant cultural change when cybersecurity is linked to the organization’s mission and impact.

Some quick high level considerations:

1. Prioritize Foundational Cyber Hygiene
   Nonprofits must first address immediate threats like phishing, patch management, and software vulnerabilities. These operational tasks are essential for mitigating common cyber risks. Implementing basic security measures such as multi-factor authentication (MFA), regular software patching, and security awareness training for staff members can significantly reduce the risk of cyberattacks. These foundational practices are vital to protecting against the most prevalent cyber threats and ensuring the ongoing functionality of nonprofit operations.
2. Develop a Phased Cybersecurity Strategy
   Nonprofits should adopt a tiered approach to cybersecurity, addressing both immediate needs and long-term goals:

   - Short-Term: focus on fixing vulnerabilities like patching systems, improving staff awareness, and setting up basic defenses such as firewalls and antivirus software.
   - Medium-Term: implement tools to assess and track cybersecurity maturity, allowing organizations to measure progress, address gaps, and move beyond basic protection.
   - Long-Term: develop a cyber-resilience strategy that includes the integration of cybersecurity into all organizational operations. A focus on continuity planning and building cybersecurity into the organization’s culture can help nonprofit organizations prepare for future risks.

3. Secure Donor and Beneficiary Data

   Protecting sensitive data, especially donor and beneficiary information, is crucial. Implementing data encryption, access control measures, and regular audits ensures that nonprofits meet data protection standards and maintain trust with stakeholders. Nonprofits should prioritize compliance with relevant regulations and invest in systems to securely store and manage sensitive information. Additionally, creating a transparent data management policy can demonstrate a commitment to privacy and security, which helps build credibility with donors and the community.
4. Raise Awareness Among Donors and Stakeholders

   It is vital for nonprofits to raise awareness about cybersecurity risks among their donors, stakeholders, and partners. Cybersecurity is increasingly seen as a strategic issue, and many donors are beginning to consider the security posture of organizations they support. By demonstrating a commitment to cyber resilience, nonprofits can foster greater trust with donors and partners. Engaging donors in the conversation about cybersecurity risks and how their contributions are being used to address these challenges can encourage more informed and strategic funding. This also involves advocating for funding opportunities dedicated to improving nonprofit cybersecurity, which can lead to stronger, more resilient organizations in the long run. See our joint open Letter to governments, corporations, and philanthropies to urge them to prioritize cybersecurity of the nonprofit sector: https://cyberpeaceinstitute.org/nonprofits-call/
5. Build Strategic Cybersecurity Partnerships

   Given the budget limitations of many nonprofits, leveraging collaborations and partnerships can provide invaluable cybersecurity support. Many cybersecurity professionals are willing to offer pro bono services, and organizations can partner with programs that provide low-cost or free assistance. Engaging with initiatives like our CyberPeace Builders program (https://cpb.ngo/), nonprofits can access expert guidance without financial burden.

Additionally, nonprofits should build strategic partnerships with other nonprofits, cybersecurity vendors, and community organizations focused on cybersecurity for common good – see NonProfit Cyber (https://nonprofitcyber.org/) and the Common Good Cyber Initiative (https://commongoodcyber.org/). These collaborations allow for knowledge sharing, resource pooling, and access to cost-effective tools and training. Nonprofits can join networks that provide shared resources and expertise, strengthening their cybersecurity posture and resilience.

Can you share an example (within confidentiality limits) of a cyber incident your organization or a partner NGO handled? What were the key lessons, and how did it shape your approach to training or preparedness?

One of our partner NGOs, providing critical services in a conflict zone, experienced a ransomware attack. The incident occurred when a staff member accidentally opened a malicious attachment in an email, which led to the encryption of vital organizational data, including financial records and sensitive beneficiary information. The attackers demanded a ransom in cryptocurrency for decryption.

Fortunately, the NGO had a backup system in place, though it wasn't fully up-to-date, resulting in the loss of several weeks' worth of operational data. The organization opted not to pay the ransom and instead restored operations from the backup. This incident revealed several vulnerabilities, including inadequate staff training, the absence of a comprehensive IRP, and insufficient data backup practices.

If I can summarize some key lessons learned:

- Staff training: the attack underscored the need for regular cybersecurity training to ensure that staff can identify and handle phishing attempts and malicious attachments effectively.
- Regular backups: it became clear that secure, up-to-date backups are essential for recovering from ransomware attacks. Nonprofits must implement robust backup strategies that allow for quick restoration of lost data.

- Incident response planning: the lack of a formalized IRP caused confusion and delays in addressing the attack. Having a clear, regularly updated response strategy is vital for minimizing damage during a cyber crisis.
- Cybersecurity as a strategic priority: the NGO recognized that cybersecurity should be integrated into their overall risk management strategy and not just as a technical or operational afterthought.

In response to this incident, the CyberPeace Institute worked closely with the NGO to improve their cybersecurity posture. Our collaborative effort included:

- Phishing simulations: we conducted phishing simulations to improve staff awareness and their ability to detect phishing attempts in real time.
- IRP: we helped the NGO develop a comprehensive IRP, ensuring all staff members understood their roles and responsibilities during a cyber crisis.
- Backup solutions: we provided guidance on implementing secure and automated backup solutions to ensure critical data can be easily restored after an attack.
- Cybersecurity culture: we emphasized the importance of embedding cybersecurity into the organization's culture, ensuring that cybersecurity awareness became a shared responsibility across all staff levels.

For more information on how the CyberPeace Institute supports NGOs in enhancing their cybersecurity resilience, you can also see our https://cpb.ngo/impact-global and Beyond125 pages. Also, in terms of attacks, a resource we recently launched is the CyberPeace Tracer – a platform that tracks cyberattacks, vulnerabilities, and threats against civil society: https://cyberpeacetracer.ngo/

Collaboration is critical in nonprofits, where teams often wear multiple hats. How do you foster cooperation between technical staff, program managers, and leadership to ensure cybersecurity is a shared priority?

We bring everyone to the table – literally. During TTXs, each participant plays their real-world role in a fictional but plausible scenario. This helps leadership understand the operational impact of their decisions, and it helps technical staff practice communicating risks clearly. When everyone sees how cybersecurity connects to their own responsibilities, they're more likely to take ownership.

To summarize a few action points:

1. **Engage Leadership in Cybersecurity as a Strategic Priority**
   For cybersecurity to be prioritized across the organization, it must be framed as a strategic issue at the leadership level. Without leadership commitment, cybersecurity efforts may lack the resources and support necessary for success.

   - Incorporate cybersecurity into risk management: leadership should integrate cybersecurity risks into the nonprofit's overall risk management framework, ensuring it's accounted for in long-term planning.
   - Set the tone from the top: leaders must advocate for cybersecurity by demonstrating its importance through decisions and modeling security-conscious behavior.

2. **Develop Cybersecurity Awareness Across All Levels**
   Cybersecurity needs to be everyone's responsibility, not just the job of technical staff. Engaging program managers and leadership in cybersecurity training ensures everyone is aware of threats and understands their role in protecting the organization.

   - Training tailored to roles: provide specialized cybersecurity training for technical staff, while offering a more general understanding of

risks and best practices for program managers and leadership.
- Make it a regular discussion: cybersecurity training should be an ongoing part of the nonprofit's culture, with updates to reflect emerging threats and evolving best practices.

3. **Foster Communication and Understanding Across Teams**
   Clear and consistent communication is a key. Technical staff, program managers, and leadership often have different perspectives – technical versus mission-focused – so it's essential to bridge this gap.

   - Regular cross-functional meetings: scheduling regular meetings between technical teams and program managers helps both sides understand each other's needs and how cybersecurity impacts operations and program delivery.
   - Create shared goals: establish joint cybersecurity goals that align with the nonprofit's mission. Emphasize that protecting data, donor information, and beneficiary privacy is critical not only from a technical standpoint but also for the organization's credibility and long-term success.

4. **Integrate Cybersecurity into Program Planning and Decision-Making**
   Nonprofits should ensure that cybersecurity is not an afterthought during program development. Program managers must understand how to assess cyber risks and integrate appropriate cybersecurity measures into their daily operations.

   - Cybersecurity champions: appoint cybersecurity champions in each department or program to act as liaisons between technical staff and program managers, ensuring cybersecurity practices are woven into all operations.
   - Include cybersecurity in project planning: cybersecurity should be considered at the onset of every project, ensuring resources are

allocated to identify and mitigate risks early in the program planning and budgeting process.

5. **Use Collaborative Tools and Frameworks**

   Collaborative tools and shared frameworks ensure that cybersecurity efforts are not siloed, helping align teams across the nonprofit.

   - Cybersecurity frameworks: nonprofits can leverage resources like the Nonprofit Cyber Solutions Index to help teams identify risks, define best practices, and track progress toward better cybersecurity.
   - Cross-departmental collaboration platforms: internal communication tools can be used to create dedicated cybersecurity channels where staff can collaborate, raise concerns, share insights, and ask questions in real time.

CyberPeace Academy also provides instruction on TTXs as part of their services. How do you adapt TTXs to address the specific needs and limitations of NGOs and nonprofits?

At the CyberPeace Academy, we know that NGOs and nonprofits face unique challenges, such as limited budgets, small teams, and diverse missions. To address these challenges, we adapt TTX to help these organizations build cyber resilience in a way that’s both effective and accessible. We keep things straightforward – no technical expertise required. The goal is to make these exercises easy to understand and practical for everyone involved. We design scenarios that reflect real-world nonprofit challenges – like an email breach affecting donor communication or a ransomware attack during a humanitarian crisis.

Our TTXs are crafted to build confidence, not to test technical skills. We use group discussions, role-playing, and realistic injects to simulate how a crisis might unfold in real time, helping participants understand their roles and how they can respond effectively.

Here’s how we adapt TTXs for NGOs:

- **Align Scenarios with Mission-Critical Activities**
  We ensure that the scenarios are directly aligned with the nonprofit's core operations. The exercises simulate events like data breaches or phishing attacks that could disrupt key activities, such as a breach of donor information or a cyberattack on the nonprofit's volunteer database. These scenarios are both realistic and relevant, based on threats commonly faced by NGOs, so participants can practice responding to incidents that directly affect their work.
- **Focus on Low-Cost, High-Impact Solutions**
  We recognize that many nonprofits operate with tight budgets, so we focus on cost-effective, practical solutions. Instead of relying on expensive tools or complex systems, we recommend simple protocols for incident reporting, basic data protection tools, and easy-to-implement measures for raising staff awareness about cybersecurity threats. The goal is to ensure that even nonprofits with limited resources can still take meaningful action to protect themselves.
- **Simplify Complexity for Non-Technical Staff**
  Given that many nonprofit teams include non-technical staff, we ensure the scenarios are designed to be understandable for everyone. We simplify the language and focus on core principles of cybersecurity, avoiding technical jargon. The scenarios include roles for all team members, from leadership to program managers, and even non-technical staff, ensuring everyone understands their responsibilities and how their actions contribute to cybersecurity.
- **Encourage Cross-Departmental Collaboration**
  Nonprofits are often cross-functional, and TTXs reflect this by encouraging collaboration across teams. Scenarios are designed to simulate how technical staff, program managers, and leadership will work together in response to a cyber crisis. This collaborative approach helps participants improve communication, coordination, and understanding of how each role contributes to the organization's cyber resilience.
- **Build Confidence Through Realistic Simulations**

We use role-playing and injects (real-time updates during the exercise) to make the simulation dynamic and engaging. This approach allows participants to respond to evolving crises and practice making decisions under pressure. The key is to build confidence, not test technical knowledge. By simulating a real-world crisis, participants learn how to respond effectively and work together to manage the situation, gaining valuable skills that will help them in actual incidents.

- **Ensure Practical, Actionable Outcomes**
  The goal of each TTX is to provide actionable insights and clear steps for improving the nonprofit's cybersecurity posture. These might include updating IRPs, identifying gaps in existing security measures, and improving cross-departmental communication.

The feedback from these exercises is used to refine the organization's approach to cybersecurity, ensuring they are better prepared for future threats and have the tools to respond effectively.

By adapting TTXs to meet the specific needs and limitations of nonprofits, we ensure these exercises are accessible, relevant, and practical, giving organizations the tools and confidence they need to respond to cyber threats in a way that aligns with their mission and resources.

What common gaps or blind spots have you observed in nonprofits during traditional TTXs, and how do you address them?

One common gap we see in many nonprofits is the lack of clearly defined incident response roles. This is something we can easily uncover during a TTX and help formalize afterward. It's less about pointing out failures and more about collaboratively identifying what's missing and how to fix it. Our approach centers on helping organizations recognize gaps and then implement practical, sustainable solutions.

Some of the main gaps/blind spots we've observed in traditional TTXs and how we address them:

- **Lack of Cross-Departmental Involvement**

The issue: many traditional TTXs focus solely on technical staff, leaving leadership and non-technical staff underrepresented. This often creates a disconnect, as leadership doesn't fully understand the operational impact of cyber incidents, and non-technical staff may feel disengaged.

How we address it: we design our exercises to include participants from all levels of the organization – technical teams, program managers, executives, and even administrative staff. This ensures that everyone, regardless of role, understands their part in responding to cyber incidents. Cross-departmental collaboration is essential, and we make sure every team member can contribute meaningfully to the crisis response.

- **Overemphasis on Technical Solutions**

  The issue: traditional TTXs often focus heavily on technical solutions and tools, which can overwhelm non-technical participants. Nonprofits may also struggle with implementing complex systems due to resource constraints, leaving them feeling excluded from the process.

  How we address it: our TTXs prioritize practical, low-cost solutions that any nonprofit can implement, even with limited resources. We focus on creating actionable, non-technical steps – such as incident reporting protocols, basic cybersecurity practices, and simple communication strategies – so that everyone can participate effectively, regardless of technical expertise.

- **Insufficient Incident Response Planning**

  The issue: many nonprofits lack a clearly defined, well-practiced IRP, and traditional TTXs often overlook this crucial element. Without a structured response plan, nonprofits can struggle to coordinate during a cyber crisis.

  How we address it: during our TTXs, we intentionally highlight the absence of a formalized response plan and collaborate with the organization to define and strengthen it. Our focus is not on pointing out mistakes but on helping nonprofits create practical, clear incident response procedures that everyone in the organization understands.

This ensures that when an incident occurs, the nonprofit can act quickly and effectively.

- **Underestimating the Role of Communication**
  The issue: communication is often neglected in traditional TTXs. While technical responses are important, nonprofits sometimes fail to recognize how crucial communication is – both internally and with external stakeholders, including donors and beneficiaries.

  How we address it: our TTXs place a strong emphasis on effective communication. We ensure that scenarios include communication with external partners and internal teams, helping participants practice how to convey critical information to stakeholders during a crisis. We also provide guidance on how to develop clear communication protocols for both donor relations and crisis management.
- **Focusing on Short-Term Fixes**
  The issue: many traditional TTXs focus on quick fixes for the crisis at hand but overlook the long-term solutions needed for building cyber resilience. This reactive approach doesn't equip nonprofits to prevent future incidents or continuously improve their cybersecurity posture.

  How we address it: we emphasize long-term cybersecurity strategies that go beyond just addressing immediate threats. After each TTX, we work with nonprofits to develop a cyber resilience plan that includes continuous staff training, ongoing threat assessments, and regular updates to security policies. This proactive approach helps nonprofits not only respond to incidents but also build a culture of cybersecurity that's sustainable in the long run.
- **Using Generic Scenarios**
  The issue: traditional TTXs often rely on generic scenarios that are not tailored to the unique needs of nonprofits. These exercises may not fully reflect the specific challenges nonprofits face, such as managing donor information or handling cyber threats during humanitarian operations.

  How we address it: we design customized scenarios that reflect the real risks nonprofits face, such as a data breach involving donor

information, a phishing attack on staff, or a cybersecurity incident during a humanitarian mission. This makes the exercises relevant and applicable, ensuring that participants are practicing responses to incidents that are directly tied to their daily operations.

Gamification is gaining traction in cybersecurity training. Do you see value in using gamified TTXs (e.g., role-playing scenarios, immersive storytelling) for nonprofits? How might this approach improve engagement or outcomes compared to conventional formats?

Absolutely! We've personally seen the difference it makes. For instance, when we ran a TTX in The Hague at the Humanity Hub, the level of engagement was incredible. People really got into their roles, and the storytelling element made the exercise not only fun but also memorable. Even our awareness training incorporates storytelling to make the lessons stick. When you remove the fear of being wrong and create an immersive experience, participants are more willing to engage, explore, and learn. This is exactly why I see such value in using gamified TTXs for nonprofits.

Gamified TTXs are a powerful tool for nonprofits, especially when it comes to enhancing engagement and improving outcomes compared to traditional training formats. Here's how gamified TTXs can drive better results for nonprofit organizations:

- **Enhancing Engagement Through Immersive Storytelling**
  Traditional cybersecurity training can often feel disengaging, especially in nonprofit settings where staff might lack technical expertise. Gamified TTXs address this challenge by incorporating immersive storytelling and role-playing scenarios. These exercises present real-world situations that are relevant to the nonprofit sector, such as an email compromise affecting donor communication or a ransomware attack during a humanitarian crisis. This approach not only captures participants' attention but also creates an emotional connection to the material, which leads to a deeper understanding and better retention of cybersecurity concepts.

- **Improving Knowledge Retention and Application**
  Studies have shown that gamified learning improves knowledge retention significantly. Active learning, a core component of gamified exercises, has been proven to increase retention rates to 75%, compared to just 5% from traditional learning methods (trainingmag.com). By simulating real-world cyber threats, participants have the opportunity to practice their responses in an engaging and dynamic environment, making them more effective in handling actual incidents. This practical experience helps ensure that participants can transfer the lessons from the exercise to real-world scenarios.
- **Promoting Collaboration and Communication**
  Nonprofits typically work with small, cross-functional teams. Gamified TTXs foster collaboration by involving participants from a range of roles – technical staff, program managers, and leadership – in decision-making. This not only promotes communication but also helps everyone understand their role in protecting the organization. Engaging participants from diverse departments strengthens the shared responsibility for cybersecurity, ensuring that security isn't seen as the sole responsibility of the technical team but a collaborative effort that is ingrained across all levels. Moreover, this cross-departmental collaboration can be particularly beneficial for diversity and inclusion. Gamified exercises allow participants from different backgrounds, including those with diverse skill sets and experiences, to engage on an equal footing. This inclusivity fosters a culture where everyone feels empowered to contribute, regardless of their technical expertise, and helps ensure that the cybersecurity strategy is comprehensive and well-rounded.
- **Measuring Effectiveness and Continuous Improvement**
  Another significant advantage of gamified TTXs is the ability to measure performance. Using points, badges, and leaderboards, participants can track their progress and identify areas where they need improvement. This data-driven approach enables nonprofits to refine

their training programs based on real-time feedback, ensuring that the focus can shift to areas that require more attention. By tracking progress over time, nonprofits can ensure continuous improvement in cybersecurity preparedness and awareness, leading to more robust defenses against emerging threats.

From your perspective, what metrics or outcomes would you prioritize to measure the effectiveness of a gamified cyber-crisis exercise for nonprofits?

Rather than focusing solely on technical outcomes, I'd prioritize measuring what participants take away from the exercise. Did they gain a clearer understanding of their roles and responsibilities in a cyber crisis? Are they more confident in their ability to respond to incidents? Have they identified gaps in communication or coordination that could hinder an effective response? In addition to these reflections, we also ask for direct feedback – What did they learn? What would they do differently next time? These insights are invaluable for shaping future trainings and ensuring continuous improvement.

I would say,

- to track participants' engagement and involvement, you can observe participation rates, time spent, and active role-playing.
- to then try to measure knowledge retention and application; it is where pre- and post-assessments are a key. Also, using scenario-based quizzes and gathering feedback post-exercise helps to determine whether participants have adopted new cybersecurity practices in their roles.
- for the actual assessment of the exercise, you can track response time, decision-making under pressure, and adherence to protocols (in case existing/given).

I think it's also very important to assess the psychological change: like asking participants to rate their confidence in responding to a cyber incident

before and after the exercise, having participants to reflect on how prepared they feel and whether they feel empowered to act during a cyber crisis, and tracking how many participants take on additional cybersecurity-related tasks or responsibilities after the exercise.

More on a long-term basis, it would be useful to monitor the implementation of changes in cybersecurity measures, such as better password management or enhanced incident reporting. Also, cyber-capacity building is a continuous effort: it is worth tracking whether participants or the organization continues to engage in cybersecurity training or drills after the exercise.

What advice would you give to other nonprofit leaders or cybersecurity professionals working in this sector to build a culture of cyber resilience despite limited resources?

Start with mindset, not money. The foundation of resilience is awareness, coordination, and commitment. You don't need a big budget to make big progress. Start with the basics: talk about cyber risks, document your processes, and run a simple TTX, even if it's just on paper. Make it relatable and mission-linked. The goal isn't perfection – it's to build awareness, improve coordination, and make sure that when something happens, people know what to do. Resilience starts with small, consistent steps. You don't need advanced tooling to make meaningful progress. Start with basic hygiene: use strong passwords, activate MFA, and keep software updated. Document who does what in a crisis. Run a tabletop drill – on paper, over a coffee, or as a part of a team retreat.

A quick list:

- **Start with the Basics: Raise Awareness and Implement Cyber Hygiene**
  Begin by discussing cyber risks openly within the organization. Implement basic security measures like MFA, regular patching, and staff awareness training on common threats. These foundational steps make a big difference in reducing risks, even with limited resources.
- **Document Processes and Create a Simple IRP**

Document key cybersecurity processes, even if they are simple. Outline basic incident response steps – who to contact, what to do first, and how to escalate. Having a clear, accessible plan is crucial for quick, coordinated action when a cyber incident arises.

- **Run Simple TTX**
  You don't need fancy tools to run a TTX. Start with a paper-based exercise that simulates a realistic cyber crisis, like a data breach. Keep it relevant to the nonprofit's mission, like donor data compromise or a ransomware attack during a humanitarian effort. The goal is to improve role clarity, communication, and coordination, not perfection.
- **Foster Cross-Departmental Collaboration**
  Cybersecurity is a shared responsibility. Encourage communication between technical staff, leadership, and program managers. Ensure everyone understands their role in a crisis and that security is integrated into daily operations across the organization.
- **Build Confidence Through Ongoing Training**
  Cyber resilience requires continuous improvement. Use simple training sessions to build confidence. Measure progress with feedback surveys and reflection on the response to the exercise. Track if participants feel more capable of managing cyber threats.
- **Leverage External Resources**
  Nonprofits can gain significant support from external platforms like Nonprofit Cyber, Common Good Cyber, our CyberPeace Builders program and Academy, which provide access to cybersecurity frameworks and expert advice. These resources help bolster internal efforts without needing significant investment.

In our view, the most effective measure is behavior change. If a team updates its crisis plan, practices quarterly TTXs, or starts including cybersecurity in strategic planning – then the exercise succeeded.

Prof. Dr. Agostino Bruzzone, University of Genoa

As Full Professor at the University of Genoa and Director of the Master Degree course in Engineering Technology For Strategy And Security (Strategos), Agostino Bruzzone has dedicated his career to advancing simulation technologies with applications spanning industry, security, and defense. With a background in mechanical engineering from the Italian Naval Academy and the University of Genoa, his work has consistently bridged academic research and real-world problem-solving, particularly in high-stakes environments. His leadership in projects like NATO's **NIAG SG60** (Simulation-Based Design and Virtual Prototyping) and the Italian Navy's **CW-SINON** (Cognitive Warfare Simulation, artificial Intelligence & Neural networks for modeling human behaviors in Operations, population and social Networks), first cognitive warfare simulator for NATO, demonstrates his pivotal role in defense innovation.

Beyond defense, Prof. Bruzzone has driven advancements in industrial optimization through partnerships with major corporations like **IBM, Fiat Group, and Ansaldo Energia**, developing cutting-edge tools for harbor security, maritime operations, and supply chain management. With over **300 scientific publications** and a legacy of cross-sector collaboration, his career embodies the transformative power of simulation in safeguarding industries and nations alike.

Dear Agostino, as an academic with strong ties to industry and government bodies, can you briefly tell us about your background and how your expertise in strategic engineering and security evolved?

Our expertise in strategic engineering developed through close collaboration with agencies, international organizations, research institutions, and companies. This synergy addressed both the digital transformation of companies, including the widespread adoption of IoT (Internet of Things), IIoT (Industrial IoT), and sensor networks generating data for advanced Data Analytics, and AI models and simulations. Simultaneously, Strategic Engineering necessitates fostering new mindsets in both young engineers and scientists, as well as in decision-makers. These individuals must be able to collaborate effectively and promptly to respond

to evolving scenarios based on the potential offered by this emerging discipline. My background has focused on modeling complex systems, particularly industrial plants, ports, manufacturing centers, and logistics networks. These contexts inherently require the ability to conduct engineering analysis across transdisciplinary subjects, with a growing emphasis on security issues and a clear understanding of the real user objectives, which is fundamental to the Strategic Engineering discipline.

How did you first get involved in TTXs, and in which industries have you applied them?

I became involved through experiences with top decision-makers to explore new concepts and evaluate the impact of emerging technologies. In the maritime sector, as the Founder and Leader of the Simulation Research Track for the NATO Science and Technology Organization, I participated in TTXs at the Centre for Maritime Research and Experimentation. Within industries, I investigated these concepts with organizations such as CSC, Boeing, and Leonardo.

Given your experience with TTXs across the maritime, logistics, and defense industries, do these sectors face any unique challenges regarding cybersecurity preparedness?

I believe these challenges are critical and often underestimated across many sectors, not just these specifically. However, the inherent complexity of the maritime, logistics, and defense sectors, involving numerous authorities and stakeholders, significantly increases their vulnerability and the potential risks posed by cyber threats.

What are some common pitfalls or limitations you have observed in traditional TTXs?

A significant pitfall is when decision-makers conduct TTXs based on intuition, sometimes influenced by overly agreeable experts. This often occurs because these experts may be primarily analysts lacking a comprehensive understanding of the interdependencies between various factors and actors, and they might possess a limited technical background in the subjects, scenarios, and processes relevant to the TTX. This can lead to

a lack of trust and the prevalence of subjective or trendy viewpoints over objective analysis.

Have you encountered situations where TTXs failed to prepare teams adequately for real incidents? If so, why?

Yes, this happens when the results suggested by a TTX are disregarded or manipulated to align with pre-existing assumptions, even when the exercise's findings indicate otherwise. This often leads to negative real-world consequences. However, such failures can also provide valuable lessons for improving future TTX approaches for the personnel involved. It is crucial to avoid superficial self-validation driven by "yes men" who simply endorse the leader's preferred or currently popular ideas.

How do you think role-playing mechanics, skill checks, and branching narratives could improve traditional TTXs?

These elements can significantly enhance player engagement and increase the level of attention among decision-makers.

Maritime security has strict regulatory and operational constraints. Could a gamified TTX model be adapted to such an environment?

Absolutely. We have conducted exercises at various levels, ranging from container yard personnel focusing on safety and security procedures to authorities and terminal/shipping companies addressing climate change and new polar routes. The stringent regulations and operational constraints are not a limitation. If the TTX is properly gamified to address specific understanding and investigation issues related to the scenario being evaluated, it can drastically improve the comprehension of mutual needs and the resolution of conflicts among different actors and players.

What types of scenarios do you believe would benefit the most from a gamified approach?

Scenarios where it is beneficial to establish a shared understanding of the situation, utilize quick, informal simulations alongside computational support to rapidly discard incorrect hypotheses, and comparatively analyze the impacts of different factors would greatly benefit. Additionally, scenarios where player engagement could be significantly enhanced through gamification would be particularly well-suited.

Finally, what advice would you give to organizations looking to enhance their incident response preparedness through better TTX design?

To identify the major risks and the historical impact of past incidents and any shortcomings in the response, and then to thoroughly explore the opportunities presented by new approaches, technologies, and principles. This involves a critical evaluation of current practices against innovative solutions to ensure that TTXs are not just theoretical exercises but realistic and effective tools for improving incident response capabilities.

PART 2
SAMPLE DOCUMENTS AND QUESTS

7
The Documents

DOI: 10.1201/9781003606314-9

With all the theoretical parts behind us, now we can focus on the relevant case studies that can provide concrete examples and inspiration for your future RPG-TTX.

As stated in the first chapter, a TTX typically lives in symbiosis with the relevant documents adopted by the organization itself. Relevant templates for the IRP and Playbooks are presented in Appendix A and B respectively, so let us see a possible actual example based on those templates that we can use later to design relevant and realistic training quest scenarios.

Our reference, fictional, company operates in the financial services sector and is named "Evil Onion Corp". It employs people for each of the Cybersecurity RPG roles seen in Chapter 4, and the following is its official IRP, based on the template proposed in Appendix A:

Incident Response Plan (IRP) for Evil Onion Corp. Version 1.0

1. Introduction

1.1 Purpose of the Plan

The IRP for Evil Onion Corp. outlines the procedures and protocols to be followed in the event of a cybersecurity incident. The objective is to ensure

a rapid and coordinated response to mitigate the impact, restore business operations, and safeguard financial data and customer assets.

(a) 1.2 Scope

This plan applies to all employees, contractors, and third-party vendors handling Evil Onion Corp.'s financial systems, customer data, and internal networks. It covers cybersecurity incidents that compromise confidentiality, integrity, or availability of Evil Onion Corp.'s digital infrastructure.

(b) 1.3 Objectives

- Rapid identification and containment of security incidents
- Efficient coordination among response teams
- Preservation of evidence for forensic analysis
- Prevention of future incidents through post-incident analysis
- Continuous training and improvement via RPG-TTX cybersecurity exercises

2. Roles and Responsibilities: Incident Response Team (IRT)

2.1 Incident Response Team (IRT)

The IRT consists of individuals with specific roles, based on the RPG-TTX system:

- **Chief Information Security Officer (CISO)** – oversees the response, communicates with executives, and ensures compliance with regulations.
- **Forensic Investigator (FI)** – analyzes digital evidence, identifies attack vectors, and provides forensic reports.
- **Red Teamer (RT)** – simulates potential attacks, advises on threat emulation, and verifies mitigations.

- **Information Security Analyst (ISA)** – coordinates initial triage, containment, and recovery operations.
- **Risk Manager (RM)** – assesses financial, operational, and reputational risks associated with incidents.
- **Legal Advisor (LA)** – ensures the organization complies with regulatory requirements and advises on legal implications.
- **HR Manager** – manages internal messaging and employee-related security concerns.
- **Network Administrator (NetAdmin)** – implements containment and mitigation strategies on Evil Onion Corp.'s infrastructure.

2.2 Contact Information

Each member of the IRT has designated primary and secondary points of contact, available in a separate secure document stored offline.

3. Incident Classification

3.1 Severity Levels

(a) 3.2 Types of Incidents

- Malware and Ransomware Infections
- Unauthorized Access (Insider or External)
- Denial-of-Service (DoS/DDoS) Attacks
- Data Breaches and Leaks
- Phishing and Social Engineering
- Compromised Credentials

(b) 3.2 Incident Reporting

Employees must report suspicious activities via the **Secure Incident Reporting Portal (SIRP)** or directly to the IRT.

4. Incident Response Lifecycle

4.1 Detection Mechanisms

- SIEM logs
- IDS
- Employee reports and phishing simulations

4.2 Initial Assessment

- Determine affected assets and data.
- Assess potential impact and escalate as needed.
- Assign an IH.

Table 7.1 Sample security levels

LEVEL	DESCRIPTION	EXAMPLES
Low	Minor incident, no operational impact	Spam emails, failed login attempts
Medium	Potential threat, limited impact	Malware infection, unauthorized access attempt
High	Major threat, operational impact	Ransomware attack, data breach
Critical	Severe crisis, regulatory and business impact	Widespread compromise, nation-state attack

5. Incident Containment and Eradication

5.1 Containment

- Isolate affected systems
- Block malicious network traffic
- Reset compromised credentials

5.2 Eradication

- Remove malware
- Patch vulnerabilities
- Validate clean system states before restoration

6. Communication and Notification

6.1 Internal Communication

- Notify employees and executives as per severity level.
- Provide clear instructions for mitigation steps.

6.2 External Communication

- Notify regulatory bodies and customers if legally required.
- Prepare public statements, if necessary.

7. Recovery and Lessons Learned

7.1 Restoration of Systems

- Validate backups and integrity before restoring operations.
- Conduct system-wide security assessments.

7.2 Post-Incident Review

- Hold a formal debrief using RPG-TTX techniques to assess response effectiveness.
- Update IRP based on findings.

8. Training and Awareness

8.1 Employee Training: RPG-TTX Integration

Evil Onion Corp. employs **Role-Playing Gamified Tabletop Exercises (RPG-TTX)** to improve cybersecurity response readiness. These exercises simulate real-world cyber incidents using:

- **Scenario-Based Exercises** – teams engage in quests that reflect real cyber threats (e.g., financial data breaches, ransomware attacks).
- **Skill-Based Challenges** – participants must roll skill checks (e.g., Incident Response, Forensic Analysis) to determine how effectively they resolve incidents.
- **Adaptive Threat Scenarios** – the CGM introduces injects based on participants' decisions and dice rolls.
- **Performance-Based XP System** – participants gain XPs for successful actions and move to more complex exercises over time.

8.2 Plan Review and Testing

- Conduct quarterly RPG-TTX exercises.
- Annual full-scale incident response drills.
- Biannual employee phishing and awareness campaigns.

9. Plan Maintenance

9.1 Document Versioning

- The IRP is reviewed semi-annually or after significant security incidents.
- The current version is maintained in a secure, offline repository.

10. Contact Information

Updated contact information for IRT members is stored securely and available only to designated personnel.

With the general IRP done, we can now move to relevant incident playbooks. We focus on three specific types of incidents and corresponding

scenarios:

- DDoS attack
- Malware infection due to phishing
- Ransomware attack

Incident Playbook: Distributed Denial-of-Service (DDoS) Attack

1. Incident Overview

1.1 Description

A Distributed Denial-of-Service (DDoS) attack occurs when multiple compromised systems flood a targeted server, service, or network with excessive traffic, rendering it unavailable to legitimate users. Symptoms include sudden unavailability of services, abnormal spikes in network traffic, and increased latency.

1.2 Objective

The primary goal is to mitigate the ongoing attack, restore services, and implement preventative measures to protect against future incidents.

2. Initial Detection and Assessment

2.1 Detection

- Alerts from Intrusion Detection/Prevention Systems (IDS/IPS)
- Network monitoring tools detecting abnormal spikes in traffic
- Reports from users experiencing service disruptions
- Cloud service provider notifications regarding excessive requests

2.2 Assessment

- Determine the scope and severity of the attack:
    - Affected services and systems
    - Source and type of DDoS attack (e.g., volumetric, application-layer, protocol-based).
- Verify if the attack is ongoing or has subsided.
- Identify attack vectors and traffic patterns.

3. Incident Response Team Activation

3.1 Team Roles

The following people need to be ready to step in:

- **CISO** (or a designated Incident Commander) – oversees response and makes executive decisions.
- **ISA** – identifies attack sources and implements mitigation techniques.
- **FI** – analyzes logs and collects intelligence on the attack.
- **RM** – assesses business impact and recommends mitigation strategies.
- **PR Specialist** (or a designated Communications Officer**)** – manages internal/external communication.

3.2 Communication Plan

- Establish an emergency communication channel for IRT coordination.
- Notify management and relevant stakeholders.
- If needed, coordinate with third-party security providers and ISPs.

4. Containment and Mitigation

4.1 Isolation

- Identify and block malicious IP addresses via firewall rules.
- Redirect traffic using a cloud-based DDoS protection service.

- If necessary, take affected services offline temporarily to prevent damage.

4.2 Mitigation

- Deploy rate limiting and filtering to block excessive requests.
- Configure load balancers and CDN services to absorb traffic.
- Activate failover mechanisms or distribute traffic across redundant infrastructure.

5. Investigation and Analysis

5.1 Forensic Analysis

- Review server and network logs to identify attack patterns.
- Analyze traffic behavior to determine botnet involvement.
- Check for IoCs linked to known attack groups.

5.2 Data Collection

- Document attack timestamps, IP addresses, and affected systems.
- Capture packet data if feasible for further analysis.
- Record mitigation actions taken and their effectiveness.

6. Eradication and Recovery

6.1 Eradication

- Ensure all attack traffic is blocked and no residual threats remain.
- Remove or update vulnerable configurations exploited by attackers.
- Patch or update security measures to harden systems.

6.2 System Recovery

- Gradually restore services, monitoring for renewed attack attempts.
- Conduct load testing to ensure stability before full-scale relaunch.
- Confirm all security systems are operational.

7. Communication and Reporting

7.1 Internal Communication

- Update management on the incident status and resolution.
- Provide a summary to affected business units.
- Conduct internal briefings on lessons learned.

7.2 External Communication

- Notify customers about service restoration (if applicable).
- Coordinate with regulatory bodies if the attack had compliance implications.
- Engage with cybersecurity partners or law enforcement if necessary.

8. Lessons Learned and Documentation

8.1 Post-Incident Review

- Conduct a retrospective to analyze response effectiveness.
- Identify gaps in detection, containment, or communication.
- Assess the organization’s readiness for future DDoS attacks by organizing an RPG-TTX exercise simulating a similar attack to reinforce learning.

8.2 Documentation

- Maintain detailed incident records for future reference.
- Update security policies based on insights gained.

- Refine monitoring and alerting mechanisms to detect early signs of future attacks.

Incident Playbook: Malware Infection via Phishing

1. Incident Overview

1.1 Description

A phishing email was successfully delivered to an employee, who subsequently opened a malicious attachment or clicked on a fraudulent link. As a result, malware has been installed on the endpoint, potentially allowing unauthorized access, data exfiltration, or further compromise of the network.

1.2 Objective

The primary objective is to identify, contain, and eradicate the malware, mitigate any potential damage, and strengthen security awareness to prevent recurrence.

2. Initial Detection and Assessment

2.1 Detection

- Suspicious activity reported by an employee or detected through automated security tools (e.g., EDR, SIEM alerts).
- Unauthorized access attempts, abnormal data transfers, or unusual system behavior.
- Alerts from threat intelligence feeds indicating a new phishing campaign targeting the organization.

2.2 Assessment

- Determine the scope of infection by analyzing affected endpoints and reviewing email logs.
- Identify whether malware has spread to additional systems or networks.
- Evaluate whether any sensitive data has been compromised.
- Classify the incident severity (Low, Medium, High, or Critical) based on impact and risk.

3. Incident Response Team Activation

3.1 Team Roles

The following people need to be ready to step in:

- **CISO** (or a designated Incident Commander) – oversees response and makes executive decisions.
- **ISA** and/or **FI** – conducts forensic investigation, analyze malware, and implement containment measures.
- **NetAdmin** – isolates infected systems, revokes compromised accounts, and restores from backups.
- **Legal Officer** – ensures regulatory requirements are met and legal risks are managed.
- **PR Specialist** (or a designated Communications Officer) – handles internal and external communication, including customer notifications if needed.

3.2 Communication Plan

- Establish secure communication channels for the IRT (avoid email if compromised).
- Notify leadership, affected users, and relevant stakeholders.
- Determine if external parties (e.g., law enforcement, cybersecurity vendors) need to be engaged.

4. Containment and Mitigation

4.1 Isolation

- Disconnect infected systems from the network to prevent malware propagation.
- Revoke credentials of affected users if credential theft is suspected.
- Block identified malicious domains, IPs, and email senders on firewalls and mail servers.

4.2 Mitigation

- Deploy security patches and updates to prevent further exploitation.
- Quarantine malicious files and analyze them for IOCs.
- Restrict access to sensitive systems until the incident is fully contained.

5. Investigation and Analysis

5.1 Forensic Analysis

- Retrieve logs from affected endpoints, email servers, and network traffic for analysis.
- Use sandboxing techniques to analyze malware behavior and determine its capabilities.
- Identify the phishing email’s origin, malicious URLs, and any attachments.

5.2 Data Collection

- Gather information on affected users, compromised credentials, and unauthorized access.
- Document malware signatures and known attack patterns for future detection.

6. Eradication and Recovery

6.1 Eradication

- Remove malware from infected systems using endpoint protection tools and forensic analysis.
- Reset passwords and reissue authentication credentials where necessary.
- Conduct full system scans and verify all traces of infection are eliminated.

6.2 System Recovery

- Restore affected systems from secure, clean backups.
- Apply hardened security controls to prevent future compromises.
- Monitor affected systems for signs of reinfection or residual threats.

7. Communication and Reporting

7.1 Internal Communication

- Inform employees about the phishing attack and steps taken to address it.
- Reinforce security awareness regarding phishing attempts.

7.2 External Communication

- If customer data is affected, notify customers and regulators as per legal obligations.
- Engage with external cybersecurity firms if further forensic assistance is required.

8. Lessons Learned and Documentation

8.1 Post-Incident Review

- Conduct a retrospective with all relevant team members to analyze response effectiveness.
- Identify gaps in phishing detection, employee awareness, and response time.
- Update security policies based on findings to enhance resilience.

8.2 Documentation

- Maintain a comprehensive report detailing the attack vector, impact, and remediation steps.
- Archive IOCs for future threat intelligence use.
- Use insights to update and improve future RPG-TTX scenarios for phishing awareness training.

Incident Playbook: Ransomware Attack

1. Incident Overview

1.1 Description

A ransomware attack has been detected on Evil Onion Corp.'s infrastructure. Attackers have **encrypted critical systems, exfiltrated sensitive data**, and **issued a ransom demand** payable in cryptocurrency. If the ransom is not paid, attackers threaten to release stolen data publicly or sell it on darknet marketplaces.

Common Indicators:

- Users reporting inability to access files due to unexpected encryption.
- Ransom notes displayed on compromised systems.
- Unusual outbound network traffic, indicating data exfiltration.

- Security alerts from endpoint protection tools or SIEM solutions.
- Failed login attempts from unusual IP addresses before the attack.

1.2 Objective

This is a challenging scenario that involves extensive actions by multiple people to coordinate an effective response across technical, legal, and PR teams. The following objectives need to be achieved:

- **Contain and mitigate** the ransomware infection.
- **Assess the scope** of encryption and data exfiltration.
- **Recover operations** securely without paying the ransom.
- **Communicate effectively** with stakeholders and regulatory bodies.
- **Implement security improvements** to prevent future attacks.

2. Initial Detection and Assessment

2.1 Detection

- Employees report ransom notes on their devices.
- SIEM system flags suspicious file modifications or mass encryption.
- Network monitoring tools detect large outbound data transfers to external IPs before encryption occurred.
- Endpoint protection systems detect unauthorized privilege escalation or execution of malicious scripts.
- Threat intelligence feeds link the attack to known ransomware groups.

2.2 Assessment

- Determine which systems are affected and isolate them immediately.
- Identify patient zero – the first compromised machine.
- Check logs for initial infection vectors (e.g., phishing email, RDP brute force, vulnerability exploitation).

- Validate ransom note details and compare with known ransomware strains.
- Estimate data exfiltration volume and type of compromised records.
- Assess whether backups are affected or remain intact.

3. Incident Response Team Activation

3.1 Team Roles

- **CISO** (or a designated Incident Commander) – oversees response strategy, coordinates internal and external communications.
- **ISA** – investigates the attack, identifies root cause, and mitigates further spread.
- **FI** – collects and analyzes evidence and determines exfiltration scope.
- **NetAdmin –** monitors and isolates compromised systems and implements firewall rules.
- **Legal Officer** – assesses compliance obligations and assists with regulatory reporting.
- **PR Specialist** – manages public messaging and press inquiries.
- **RM** (or Business Continuity Manager) **–** evaluates ongoing situation and ensures minimal disruption to critical operations.

3.2 Communication Plan

- **Internal:** Regular briefings between IT, security, executive leadership, and legal teams.
- **Regulatory Bodies:** If data breach laws apply (e.g., GDPR, PCI-DSS, CCPA), notify relevant agencies.
- **External Partners:** Notify affected vendors or third-party service providers.
- **Public Disclosure:** If customer data is impacted, issue a **controlled public statement** through PR channels.

4. Containment and Mitigation

4.1 Isolation

- Disconnect infected systems from the corporate network.
- Block outbound traffic to attacker-controlled IPs.
- Revoke compromised credentials and enforce multi-factor authentication (MFA).
- Disable remote access tools (e.g., RDP, VPN) for compromised accounts.

4.2 Mitigation

- Identify C2 servers and block them at the firewall level.
- Restore a clean environment by deploying backup infrastructure.
- If live forensic analysis is required, keep infected systems powered on but disconnected.
- Deploy EDR tools to monitor suspicious activities.

5. Investigation and Analysis

5.1 Forensic Analysis

- Identify malware strain and ransomware group affiliation (e.g., LockBit, BlackCat, Clop).
- Analyze attack kill chain using MITRE ATT&CK framework to track attacker movement.
- Examine compromised user accounts and detect privilege escalation methods.

5.2 Data Collection

- Preserve system logs, firewall logs, and endpoint security telemetry.
- Review file modification timestamps to estimate encryption timing.

- Verify data exfiltration paths and destinations.
- Capture ransom note metadata to determine attacker communications methods.

6. Eradication and Recovery

6.1 Eradication

- Remove malware artifacts, persistence mechanisms, and backdoors.
- Reset compromised credentials and enforce strict password policies.
- Apply security patches to exploited vulnerabilities.
- Conduct full AV/EDR scans across all systems before reconnecting them.

6.2 System Recovery

- Restore affected systems from clean backups (ensure no reinfection risk).
- Implement segmentation controls to isolate critical business systems.
- Conduct validation testing to confirm systems function properly.
- Reintegrate recovered assets into production gradually to monitor anomalies.

7. Communication and Reporting

7.1 Internal Communication

- Provide executive leadership with a situation report.
- Inform employees of security policy updates and required actions.
- Issue a security advisory to reinforce phishing awareness training.

7.2 External Communication

- If regulated data was exposed, notify regulatory agencies within required timelines.
- Provide affected customers with breach details and remediation steps.
- If necessary, engage law enforcement (e.g., FBI, Europol, national cybersecurity agencies).
- Craft public statements addressing the attack without disclosing operational weaknesses.

8. Lessons Learned and Documentation

8.1 Post-Incident Review

- Analyze root cause and incident response gaps.
- Review why detection mechanisms failed and where response time can improve.
- Update threat intelligence sources with IoCs.
- Refine incident playbooks for faster execution in future cases.

8.2 Documentation

- Maintain an incident report with technical details and executive summary.
- Document security control failures and recommended improvements.
- Develop new security policies to mitigate identified weaknesses.

Final Notes on Ransom Payment Consideration

- Ransom payment is NOT recommended as it does not guarantee full recovery and may encourage future attacks.
- Legal and regulatory risks must be considered before engaging with attackers.
- If decryption is necessary, explore law enforcement resources or security research decryptors.

Next Steps:

1. Implement long-term security controls such as zero trust architecture and enhanced email filtering.
2. Develop cyber insurance coverage policies with explicit ransomware clauses.
3. Enforce continuous employee security awareness training to reduce phishing success rates.

These sample documents can be used together with the following chapters to practice simple stand-alone exercises or customized and expanded by incorporating an organization’s specific tools and procedures, creating tailored scenarios.

8

The Great Blackout

A DDoS Crisis

DOI: 10.1201/9781003606314-10

As discussed in Chapter 5, whenever creating a scenario to practice readiness under specific circumstances, we have to be sure the setup is as realistic as possible. In the previous chapter we also defined the core documentation for our fictional “Evil Onion Corp.”, including the general IRP and a few specific playbooks. We can assume the team has access to them and know them or, at least, they are aware of them and know how to access them for reference. Any quest we create needs to strengthen the learning and understanding of all the procedures discussed in there and, eventually, provide additional insights for further improvements.

As a first test-case scenario, let’s imagine our company is under a DDoS attack. Ideally, as stated in the corresponding playbook, in this scenario the following team members should take part in the exercise:

- CISO
- ISA
- FI
- RM
- PR Specialist

The quests we are going to design should be based on a few real attacker's TTPs from the MITRE ATT&CK framework so that the scenario evolves logically, and then naturally directs the team to comply to their respective duties by following the IRP and the relevant playbook. The quest should also give room to possible mistakes and failures, which will be determined by skill checks with suitable DCs thresholds that take into account the specific abilities of the team members. Injects with unexpected turn-arounds should also be planned wherever possible to keep things unpredictable, especially in case of a skill check failure.

The Quest

This tabletop RPG scenario is designed to test the IRT against a realistic DDoS attack using MITRE ATT&CK techniques. The team must follow the IRP and Playbook, making strategic decisions and rolling skill checks to determine outcomes. The session is structured to last 1.5–2 hours and includes injects to simulate unexpected challenges. Remember to award XP accordingly for every successful skill check.

Let's begin!

Evil Onion Corp.'s online banking platform has gone offline due to a massive multi-vector DDoS attack. Customers report being unable to log in, and social media backlash is growing. The team must detect, mitigate, and recover while managing RD. The attackers are a well-organized threat group known as "Void Echo", which specializes in ransom-based DDoS.

Their TTPs align with MITRE ATT&CK, particularly:

- T1498.001: Direct Network Flood[1]
- T1498.002: Application Layer Flooding, Reflection Amplification[2]
- T1499: Endpoint DoS[3]
- T1583.005: Use of Botnets[4]

The players must work collaboratively to detect, mitigate, and recover from this attack while facing injects and consequences based on relevant skill

checks.

Here, the CGM needs to monitor two relevant business metrics:

- RD, starting at zero, will increase when certain skill checks fail, escalating the attack.
- Financial Damage due to Disruption (FDD), estimated in $100,000 per hour of disruption.

At the end of the exercise, these will provide some hard numbers for the team to think about.

Act 1: The Calm Before the Storm (Detection Phase)

The CGM can set up the scenario by explaining the following symptoms:

- Customer complaints about slow transactions and login failures.
- SIEM alerts show a spike in TCP SYN requests.
- Unusual DNS query volume detected.

How should the team react? Remember that the CGM and the team need to reference:

- IRP
    - Sections 3.1 and 3.2: Incident Classification
    - Sections 4.1 and 4.2: Detection Methods
- DDoS Playbook
    - Section 2.1: Detection
    - Section 2.2: Assessment

Skill Checks:

ISA: Roll **Threat Analysis (DC 14)** to analyze logs.

- **Success:** Identifies SYN Flood traffic from suspected botnets.
- **Failure:** Misinterprets as routine traffic surge, delaying mitigation. Add $200,000 to FDD.

The ISA, or another team member with TA > 12, can roll a second time and be awarded XP if successful, but the aforementioned penalty applies in case of any additional failure. If two or more failures, RD also increases by 1.

FI: Roll **Forensic Analysis (DC 12)** to check historical patterns.

- **Success:** Confirms a botnet-origin attack from over 100K IPs.
- **Failure:** Cannot determine source, delaying ISP coordination. A Layer 7 HTTP flood cripples login pages, increasing user complaints. RD is increased +1. Add $100,000 to FDD.

If either check fails, **Stress Management** skill for the whole team takes a –1 penalty for the rest of the exercise.

The team now needs to discuss incident type and classification. Award 1 XP to all team members if the classification sounds correct.

Act 2: Full-Scale Attack (Response Phase)

The threat escalates and the following information is to be reported to the team:

- 50Gbps+ volumetric attack hits core servers.
- Attackers issue a Bitcoin ransom demand to stop the attack.
- Fake “data breach” claims appear on social media.
- Consequences: RD +1, FDD + $100,000.

Ask the team how they would proceed according to documentation. In particular:

- IRP Section 5.1: Containment
- IRP Sections 6.1 and 6.2: for Internal and External Communication

- Playbook Section 3.2: Communication Plan
- Playbook Sections 4.1 and 4.2: for mitigation tactics

This should lead to the following actions **Skill Checks:**

CISO: Roll **Stakeholder Engagement (DC 16)** to organize and coordinate response.

- **Success:** ISP agrees to deploy geofencing and rate-limiting.
- **Failure:** Negotiations stall, prolonging downtime. Add $100,000 to FDD.

RM: Roll **Risk Assessment (DC 15)** to prioritize assets.

- **Success:** Focuses defense on **critical financial services** (RD-1).
- **Failure:** Overloads mitigation resources, causing longer recovery. Add $100,000 to FDD.

PR Specialist: Roll **Stress Management (DC 14)** to manage media crisis.

- **Success:** Reassures customers, **minimizing panic** (RD –1).
- **Failure:** Narrative spirals out of control, **damaging reputation** (RD +2).

Inject: If PR Specialist check fails, stock value drops 5% and regulators demand an explanation, which the PR needs to draft if a template is not already available.

Act 3: Recovery and Aftermath

After geofencing and rate-limiting are implemented, traffic stabilizes but residual botnet traffic persists.

- Forensic analysis is now required to trace attack origin.
- Regulatory compliance reporting needs to be initiated.

Here the team needs to reference DDoS Playbook Section 5 (Investigation and Analysis) and Section 6.2 (System Recovery) for operational restoration.

Skill Checks:

FI and/or **ISA:** Roll **Threat Analysis (DC 15)** to analyze botnet.

- **Success:** Identifies attack as **IoT-driven**.
- **Failure:** Skill check needs to be repeated. Add +$100,000 to FDD for each failure.

PR Specialist or **CISO** or **RM (character with higher LDR skill goes first):** Roll **Policy Compliance (DC 16)** to verify all reporting duties have been performed correctly.

- **Success:** RD is ultimately contained (RD -1).
- **Failure:** Evaluate possible RFs according to specific legislative environment (RD +2).

Last, the team needs to discuss, according to IRP Section 8.1, any relevant lesson learned. Was there any area in the documentation that was not clear? Did team members know what to do or were they confused at any time? If so, why?

If any relevant point is noted, each team member is awarded +2 XP.

At the end of the session, the CGM evaluates performance according to the original RD and FDD metrics.

- RD less than 3, FDD less than $300,000: Attack mitigated quickly, minimal RD. Each team member is awarded 5 XP.
- RD less than 5, FDD less than $500,000: Some downtime, minor loss of customer trust. Each team member is awarded 3 XP.
- RD less than 7, FDD less than $800,000: significant financial and reputation losses. Each team member is awarded 1 XP.

- RD greater or equal than 7, FDD greater or equal than $800,000: Major operational failure. No XP awarded.

Comments and Additional Ideas

It should be clear by now that a successful RPG-TTX session is not just about following a linear script. It is about engaging participants, creating meaningful challenges, and ensuring useful learning outcomes. Like a traditional GM in a pen and paper RPG, the CGM needs to wear different hats and act as a narrator, adversary, and moderator, adjusting the scenario dynamically based on the ongoing team performance.

One of the CGM's most important responsibilities is adapting the difficulty curve. If the ISA quickly identifies the SYN Flood in Act 1, the CGM might escalate the attack by introducing injects about a second wave with randomized IP rotations, forcing the team to explore and deploy more advanced countermeasures. Conversely, if the team struggles early on, the CGM could introduce an in-game prompt from a third-party security vendor offering insights, giving them a much-needed nudge in the right direction but adding some additional financial impact.

Unexpected injects keep players on their toes. For example, if the PR Specialist successfully handles media fallout, the CGM could introduce an anonymous whistleblower claiming the company has been negligent in past security audits. How could the team react to this? Maybe they would need to pivot from technical mitigation to crisis management, testing their ability to manage reputational risk and regulatory scrutiny under additional pressure. If the RM misallocates mitigation resources, the CGM could trigger a secondary infrastructure failure, such as database timeouts impacting backend processing, adding a layer of technical complexity to the scenario.

The CGM should also observe how well the team follows the IRP and Playbook. If players rely too much on improvisation instead of referencing documented procedures, the CGM can trigger some form of additional penalty, for example, delaying mitigation efforts due to confusion about

response roles. Alternatively, if players adhere to protocols effectively, the CGM can reward them with operational advantages, such as an early warning from a threat intelligence partner about the attack's origins or simply assign additional XP.

Another critical role of the CGM is adjusting role-based impact. If the CISO makes strategic decisions without consulting the ISA, the CGM might introduce flawed mitigation tactics, leading to service degradation despite successful filtering. This reinforces the importance of cross-functional collaboration. If players skip key forensic steps, the CGM could introduce an audit requiring a full retrospective investigation, delaying recovery efforts further or perhaps adding some RF.

Finally, pacing is crucial. The CGM should ensure the exercise remains engaging without rushing through key decisions and stays within the planned timeboxed duration. If players stall, the CGM can introduce time pressure elements, such as a regulatory deadline for incident reporting, forcing quicker decision-making. Conversely, if players are moving too quickly without considering alternatives, the CGM might introduce a misleading clue or false positive, encouraging a deeper analytical approach. In other words, each scenario is just a trace, a canvas that the CGM needs to draw upon and improvise with as the "adventure" unfolds.

Notes

1. https://attack.mitre.org/techniques/T1498/001/ ⏎
2. https://attack.mitre.org/techniques/T1498/002/ ⏎
3. https://attack.mitre.org/techniques/T1499/ ⏎
4. https://attack.mitre.org/techniques/T1583/005/ ⏎

9

The Silent Intruder

A Spear-Phishing APT Attack

DOI: 10.1201/9781003606314-11

Phishing and, more importantly, spear-phishing, that is, an informed and targeted attack based on some acquired knowledge of the potential victim, is an increasingly concerning trend due to advancement in AI as well as the facility to find out information on almost anyone via Open Source Intelligence (OSINT) techniques. Most modern attacks targeting businesses and organizations of all sizes do, indeed, start via an apparently innocuous email sent to an unsuspecting employee who, inadvertently, sets into motion a catastrophic series of events by simply clicking on a link or opening an attached file.

To explore how Evil Onion Corp.'s defensive strategy may react under such circumstances, let's design a new quest that, besides the IRP, references the "Malware Infection via Phishing" Playbook presented in Chapter 7. Accordingly, the following team members should be involved:

- CISO
- ISA
- FI
- NetAdmin
- Legal Officer

- PR Specialist

As this RPG-TTX scenario wants to present a high-stakes incident, requiring a cross-functional response team while tracking financial, legal, and reputational impact, always keep in mind that the CGM should adjust difficulty based on player performance and starting level (i.e., if the team members have already acquired enough XP to be promoted to level 2 or higher, DC values can be set higher or more severe consequences and injects can be added).

Now, let the game begin. Are you ready?

The Quest

The Evil Onion Corp. IRT has unknowingly been under cyber siege for two months following a successful spear-phishing attack. An employee in the finance department, believing they were opening a PDF invoice from a trusted client, inadvertently triggered a Remote Access Trojan (RAT). This allowed a yet unknown Advanced Persistent Threat (APT) group to infiltrate the network, maintain persistence, and slowly exfiltrate sensitive financial and strategic data.

The attackers, using MITRE ATT&CK techniques, carefully moved laterally, evaded detection, and established multiple backdoors. Their presence has only now been partially detected when a security alert flagged unusual outbound traffic from an internal file server. The IRT must now assess, contain, and eradicate the threat while minimizing damage to financials, reputation, and regulatory standing.

This is 1.5–2-hour exercise and will challenge team members through technical analysis, strategic decision-making, and crisis management. Their actions will impact the company’s regulatory exposure and public perception. Mistakes or delays may allow the attackers to cover their tracks, reinfect systems, or leak stolen data.

Accordingly, the following business metrics will be tracked:

- RD, as more sensitive data gets leaked.
- Recovery Costs (RC): initial forensic costs at $300,000, increasing whenever a containment step fails.
- RF, as the company's practices get audited and questioned due to delays.

The Threat Actor is a mysterious APT Group specializing in long-term breaches and the following MITRE ATT&CK TTPs have been referenced to create this scenario:

- T1566.001: Spear-Phishing via Malicious Attachment[1]
- T1204.002: Execution of Malicious Files[2]
- T1071.001: C2 Communication via Web Protocols[3]
- T1021: Remote Services: Lateral Movement via Valid Accounts by using different techniques and tools[4]
- T1074.001: Data Staging for Exfiltration[5]
- T1041: Data Exfiltration over C2 Channel[6]

Act 1: A Flare in the Dark (Detection Phase)

- The ISA receives an alert from the SIEM flagging unusual outbound traffic from a file server to an external IP linked to known APT activity.
- The NetAdmin notices persistent RDP connections to critical systems outside of working hours.
- Internal data integrity checks reveal files being compressed and duplicated in unexpected locations.

How should the team react? Reference:

- IRP
    - Section 3: (Incident Classification)
    - Section 4.1: (Detection Methods) for identifying anomalies

- Malware Infection via Phishing Playbook
    - Section 2: (Initial Detection and Assessment)

Skill Checks:

ISA or **FI (the one with higher TA rolls first):** roll **Forensic Analysis (DC 15)** to analyze network logs.

- **Success:** The check correctly identifies consistent **C2 beaconing** every **4 hours**, correlating with **known RAT behaviors**.
- **Failure:** Attributes the traffic to **misconfigured backup services**, delaying the response by 6 hours. This delay will add +$300,000 to RFs. If the first team member fails, a second one can step in and roll again, adding a penalty of RD+1 in case of failure.

NetAdmin or **ISA (whoever has higher TA rolls first):** Roll **Incident Response (DC 14)** to trace unauthorized remote logins.

- **Success:** Discovers compromised **user credentials** linked to a **finance employee's laptop**.
- **Failure:** Mistakes activity for an **internal IT audit**, delaying containment. Add +$300,000 to RF. Another team member can roll again to double check, adding $200,000 to RC if failing once again.

Injects: If either check fails, the CGM can decide to roll (DC 10) to see whether the attackers use the additional delays to escalate privileges on another compromised machine, allowing them to install a second-stage payload, increasing exfiltrated data volume by 30%. If so, a D20 roll should determine the outcome:

- 1: Add +2 to RD and $200,000 to RC.
- 2–10: Add +2 to RD.
- 11–20: Add $200,000 to RC.

As this first stage of assessments unfolds, any team member can (and should) step in and discuss the severity level of the ongoing incident. This should be classified as a “High” impact incident according to the IRP. The first team member who classifies the incident correctly is awarded 1 XP.

Act 2: Trapped in the Web (Response Phase)

As more details on the ongoing attack emerge, it becomes apparent that the attackers have been exfiltrating sensitive financial and legal documents.

- The legal team begins receiving whispers from journalists about a possible data breach leak.
- Thanks to privilege escalation, attackers managed to modify firewall rules, allowing persistent outbound traffic even if C2 nodes are blocked.

At this stage, the team needs to reference:

- IRP
    - Section 5: (Containment Strategies) for isolating threats
    - Section 6.2: (External Communication)
- Playbook
    - Section 4: (Containment and Mitigation)
    - Sections 3.2 and 7: (Communication Plan and Reporting) for breach reporting policies

Skill Checks:

FI: Roll Forensic Analysis (DC 16) to analyze file transfers and identify exfiltration patterns.

- **Success:** Pinpoints exact timestamps, attack vectors, and staging directories, making containment much easier.
- **Failure:** Overlooks hidden exfiltration scripts, allowing continued data theft (RD +1, RF+$200,000).

If the FI fails, other team members with **TA > 12** should try as well, but they should roll **Stress Management (DC 12)** instead. If successful, this will keep RD under control (RD-1). On the other hand, an additional $100,000 in RF per failure should be added. If someone fails here, the whole team Stress Management bonus will be reduced by 1 for the duration of the exercise.

CISO: Roll **Policy Compliance (DC 17)** to manage containment efforts across departments.

- **Success:** Initiates an isolation plan without disrupting critical operations.
- **Failure:** Shuts down too many systems at once, impacting company-wide productivity (RD+2, RC+$250,000).

Legal Officer: Roll **Policy Compliance (DC 15)** to determine **reporting obligations**.

- **Success:** Advises timely notification to regulators, minimizing penalties (RD-1, RF-$200,000).
- **Failure:** Delays decision-making, leading to fines and compliance scrutiny (RF+$300,000).

If the Legal Officer fails, the **CISO** can step in and do the damage control. Roll **Stress Management (DC 15)**.

- **Success:** Regulators are still notified within an acceptable time frame (RF-$300,000).
- **Failure:** The situation is getting chaotic and may get out of hand.

If both the Legal Officer and the CISO fail, a government official announces an investigation, significantly reducing public trust (RD+3) and increasing RFs (RF+$500,000).

Act 3: Cutting the Strings (Eradication and Recovery)

As we approach the end of the incident, the attackers, realizing they have been detected and effective countermeasures are being taken, attempt a final mass data dump before abandoning their foothold. Can the team keep their attention high despite the increased stress?

Remember the team can breathe a final sigh of relieve only once all the remaining backdoors have been eradicated, all the relevant forensic evidence has been analyzed and all systems have been restored securely.

At this stage, the team should reference the following:

- IRP
    - Section 5.2: (Eradication)
    - Section 6.2: (External Communication) for any additional statement
    - Section 7: (Recovery and Lessons Learned) for strengthening defenses
- Playbook
    - Section 6: (Eradication & Recovery) for cleaning compromised systems
    - Section 7: (Communication and Reporting) for dealing with any eventual regulatory request

Skill Checks:

ISA, NetAdmin or **FI (to roll according to their RES score, highest goes first):** Roll **Stress Management (DC 13)** to figure out the last attempt by

the hackers to exfiltrate additional data.

- **Success:** the hacker's attempt to establish a new connection and leak additional data is identified by proper analysis of network traffic. Proper countermeasures are taken.
- **Failure:** In the heat of the confusion, the new malicious connection and outbound traffic is overlooked. More data is leaked. CGM to roll 1D20 for damage:

    - 1: RD+1, RF+100,000, RC+$100,000
    - 2–8: RD+2
    - 9–14: RF+$200,000
    - 15–20: RC+200,000

Once a specific damage has been declared and recorded, this skill check can be repeated by another team member till passed.

Things seem to slow down now, but some dangers may still be lurking in the shadows …

FI or **ISA (whoever has higher RES rolls first):** Roll **Threat Analysis (DC 15)** to uncover lingering persistence mechanisms.

- **Success:** Finds hidden scheduled tasks and unauthorized admin accounts, removing all backdoors.
- **Failure:** Misses one backup persistence method, allowing attackers to attempt re-entry in the future. Who knows when the nightmare will start all over again?

If first player fails but second player succeeds: The next time this or a similar RPG-TTX is run, all team members will take a -1 penalty to their Stress Management bonus.

If both players fail: Besides the previous penalty, at the end of the exercise, XP gained is halved for each team members.

Once the technical side of things appears under control:

PR Specialist: Roll **Stakeholder Engagement (DC 14)** to control media backlash.

- **Success:** Frames the breach as well-handled, minimizing reputation damage (RD-2).
- **Failure:** Fails to manage public perception, causing a customer exodus (RD+3).

Either way, the exercise is completed. Congratulations!

As we wrap things up, we should also check whether the team managed to limit the various possible penalties and award extra XP to reward a significant achievement in limiting damages.

- If RD is less than 4, award 2 XP to each team member.
- If RF amount to less than $500,000, award 2 XP to each team member.
- If RC amount to less than $300,000, award 2 XP to each team member.

If the costs instead went out of hand … well, this should give the team more food for thought and realize how even a small indecision can have very serious consequences!

Comments and Additional Ideas

This TTX should help revealing both strengths and weaknesses in the organization's readiness, incident detection, response coordination, and crisis management capabilities. In fact, in a real scenario it is fundamental for the team to identify the signs of an ongoing attack as quickly and early as possible and, by going through this exercise, the CGM can have an opportunity to evaluate, and eventually address, the following points:

- How well the team identified the initial compromise.
- Whether containment efforts prevented further escalation.
- If legal and PR actions managed to minimize external damage.
- Whether backdoors and attacker footholds were fully eradicated.

While the team successfully identified and contained the breach in the end, delays in detection and communication breakdowns could, in fact, significantly increase the damage incurred. Going through the exercise should reinforce the awareness that modern cybersecurity incidents are not just technical problems anymore, but they are organizational crises requiring interdisciplinary coordination.

As cyber threats continue to evolve, our TTX scenarios cannot remain still either and need to evolve too, by taking into account the latest TTPs identified by knowledge bases such as MITRE. This means that, as the team gets more experience both in real life and in terms of XP points in our gamified system, follow-up exercises should introduce more complex adversary tactics, possibly integrating supply chain security challenges, for example, and test the organization's resilience against simultaneous multi-vector attacks. Would everyone know what to do and be aware of the pressure they would face in such situations?

In any case, once the exercise concludes, it is crucial to reflect on the challenges encountered, the decisions made, and the overall effectiveness of the team's response. Unlike the previous exercise, this APT scenario aimed at emphasizing the long-term stealth and persistence of an adversary. As such, one of the most critical takeaways for the team should be the realization that attackers may not just infiltrate into a network but hide for several weeks or even months before any anomalies were detected. This highlights the importance of continuous monitoring for any possible anomalies and proactive threat hunting rather than relying solely on reactive measures.

When doing any sort of exercise retrospective, the CGM should keep in mind specific moments and events. For example:

- The detection check to uncover a lingering presence of the attackers was a critical moment. If this check had failed, the attackers would have remained undetected even longer, further increasing the RD and RFs from the breach. In a real scenario, this may imply that the team's reliance on standard IDS/IPS alerts and SIEM logs alone may not be

enough for a proactive defense, and the absence of a deeper traffic analysis looking for behavioral anomalies may effectively delay recognition of data exfiltration patterns, allowing the adversary to exfiltrate even more sensitive materials undetected.

- The intersection between technical response and legal/regulatory obligations proved also to be a recurring challenge throughout the exercise, providing opportunities for discussing how the incident response is not solely a technical challenge but requires an interdisciplinary approach with clear lines of communication between technical and non-technical teams. The Legal Officer's regulatory compliance check determined whether reporting deadlines were met or not. If this failed, RFs and legal liabilities increased significantly, while the PR Specialist's crisis communication check directly impacted how the media and stakeholders perceived the breach. Poor handling here would likely lead to greater RD, affecting the whole company.
- Management was also under pressure. The CISO's leadership and strategic thinking were tested in making critical decisions. When the team lacked a clear chain of command, confusion arose, leading to unnecessary delays and inefficient task delegation, stressing once again that decision-making, team dynamics, and leadership effectiveness is critical.

From a practical perspective, if relevant to the specific organization, more technical nuances can be added when discussing the adversary's ability to move laterally across the network and escalate privileges undetected. This gives an opportunity to check for possible weaknesses in the organization's network segmentation, access control policies and, eventually, in any zero-trust architecture implementation, which can be discussed in detail during the exercise retrospective.

Notes

1. https://attack.mitre.org/techniques/T1566/001/ ⏎
2. https://attack.mitre.org/techniques/T1204/002/ ⏎
3. https://attack.mitre.org/techniques/T1071/001/ ⏎
4. https://attack.mitre.org/techniques/T1021/ ⏎
5. https://attack.mitre.org/techniques/T1074/001/ ⏎
6. https://attack.mitre.org/techniques/T1041/ ⏎

10
To RDP or Not to RDP? A Ransomware Crisis

DOI: 10.1201/9781003606314-12

To conclude, let's focus on a quest dedicated to the scariest possible attack of today, affecting as many as 73% of businesses globally in 2023:[1] ransomware. As the name suggests, ransomware is a type of attack that encrypts all systems it infects, making them unusable unless an expensive ransom, usually in the form of cryptocurrencies, is paid to the cybercriminal gang.

As this is a particularly complex scenario, several people may be involved in the training process. From our playbook, we know the following team members should be involved:

- CISO
- ISA
- FI
- NetAdmin
- Legal Officer
- RM
- PR Specialist

As usual, we will rely upon established TTPs from the MITRE ATT&CK framework. Note that not all situations and events hypothesized here may be applicable within a real setting. Nonetheless, they should still provide food for thought to make relevant team members think about possible potential pitfalls and plan for alternative solutions.

The Quest

This tabletop RPG scenario simulates a realistic ransomware attack against Evil Onion Corp. using MITRE ATT&CK techniques. The IRT must follow the IRP and Ransomware Playbook, making strategic decisions and rolling skill checks to determine outcomes. As the scenario unfolds, the company may incur in increasing revenue losses (RL), RDs, RCs, and RFs.

The exercise should take 1.5–2 hours and will include injects that introduce new challenges based on team performance, and it is built around the following MITRE ATT&CK TTPs:

- T1078.003[2] and T1078.004:[3] Valid Accounts – Local and Cloud
- T1133:[4] External Remote Services (RDP Exploitation)
- T1486:[5] Data Encrypted for Impact (Ransomware Deployment)
- T1567.002:[6] Exfiltration Over Web Service
- T1587.001:[7] Customized Malware

Scenario Premise

A senior employee's RDP credentials were found on the dark web and used to access Evil Onion Corp.'s internal financial systems. The attacker exfiltrated highly sensitive financial and client data before deploying ransomware, encrypting key databases, email servers, and payment processing systems. The attackers, claiming to be from the nefarious Rainbow Moth Ransomware Group, demands $8.88 million in Bitcoin to restore access.

Throughout the exercise we will monitor the following damage metrics:

- RL, increasing as the systems remain unusable.
- RD, as more sensitive data gets leaked.
- RF, if procedures are not followed properly.
- RC, increasing as more workstations and servers get encrypted.

Act 1: Silent Intrusion (Detection and Initial Response)

Discuss the following symptoms to set up the scene:

- System administrators report unusual login patterns (off-hours RDP access from an unrecognized IP address).
- Finance team is locked out of critical databases.
- SIEM alerts indicate large outbound data transfers overnight.

How should the team react? Reference:

- IRP
    - Section 3: (Incident Classification)
    - Section 4.1: (Detection Methods) for identifying anomalies
- Ransomware Playbook
    - Section 2: (Detection)
    - Section 4.1: (Isolation) for rapid response procedures

Skill Checks:

ISA or **NetAdmin (if TA > 12):** Roll **Threat Analysis (DC 14)** to analyze SIEM logs.

- **Success:** Identifies unauthorized RDP session and traces IP address.
- **Failure:** Misinterprets as a VPN misconfiguration, delaying threat containment. RL +$100,000, RC +$50,000.

FI or **ISA (if TA > 13. Team member with higher TA rolls first):** Roll **Forensic Analysis (DC 15)** to confirm data exfiltration.

- **Success:** Detects stolen financial records uploaded to **anonymous cloud storage**.
- **Failure:** Misses evidence, allowing attackers to sell data undetected (RD+2).

NetAdmin: Roll **System Configuration (DC 14)** to isolate compromised machine.

- **Success:** The compromised account is confirmed and its access removed. Additional lateral movement, as well as possible privilege escalations, is prevented.
- **Failure:** Important details are missed. RDP port is left open, allowing further exploitation (RL +$200,000, RC +$50,000).

Inject: If both checks fail, attackers deploy a second payload, encrypting additional infrastructure: RC +100,000, RD +3. Stress Management for the whole team: −2.

As this first stage of assessments unfolds, any team member can step in and discuss the severity level of the ongoing incident. This should be classified as a “High” impact incident according to the IRP. The first team member who classifies the incident correctly is awarded 1 XP.

Act 2: Full-Scale Lockdown (Decision-Making, Response and Initial Recovery)

Unfortunately, the situation escalates quickly:

- A ransom note appears on all affected systems demanding $8.88 million in Bitcoin.
- Attackers claim to have leaked client financial data to dark web forums.

- Regulatory bodies request an immediate impact assessment.

Now the team needs to look into the following:

- IRP
    - Sections 5.1: (Containment)
    - Sections 6.1 and 6.2: for internal/external stakeholder messaging
- Ransomware Playbook
    - Section 3.2: (Communication Plan)
    - Section 4: (Containment and Mitigation)

Skill Checks:

CISO: Is the CISO on top of things? CGM should prompt CISO on next course of action based on available documents. If answer is satisfactory, award +1XP. In any case, after discussion, roll Stress Management (DC 15) to determine the next course of action in the simulation.

- **Success:** Leads a coordinated effort, prioritizing recovery and damage control (RD: -1).
- **Failure:** Hesitates, delaying response and worsening financial losses (RL +$200,000).

Legal Officer: CGM to ask what regulations the company needs to follow under these circumstances. Award +1 XP if answer is satisfactory. Then roll **Policy Compliance (DC 15)** to assess regulatory risks.

- **Success:** Advises on proper disclosure protocols to regulators.
- **Failure:** Misinterprets requirements, leading to fines for late disclosure. Regulators launch an investigation, adding $500,000 in fines and legal fees (RF).

RM: How would he evaluate the current and prospective financial impact? Award +1 XP if answer is satisfactory. Then roll **Risk Assessment (DC 14)** to evaluate financial impact for the exercise.

- **Success:** Provides accurate monetary projections for leadership.
- **Failure:** Underestimates damage, affecting decision-making (Stress Management: −1). The team is under additional pressure.

How would the **PR Specialist** handle the situation? Ask (+1XP if answer is satisfactory), then roll **Stakeholder Engagement (DC 14)** to manage the outcome.

- **Success:** Controls media narrative, minimizing reputation damage (RD –1).
- **Failure:** The public statement is not convincing. Public panic increases and several important clients flee (RD+3, RL+$1,000,000).

Now it is for the technical people to step in for the containment and mitigation phase (e.g., Ransomware Playbook Section 4.2). Anyone among the **ISA**, the **FI**, and the **NetAdmin**, as long as they have TA > 10, can be prompted with the next rolls and actions.

What would they do? The first who can draft the right course of action gets +1 XP.

Do note that now the team is under string pressure. Stress management should be included in these rolls, whether it has a positive or negative value.

Roll for **Forensic Analysis + Stress Management (DC 15)** to block the ongoing infection:

- **Success:** The C2 servers used by the attackers are correctly identified and additional rules to the firewall are added to block any communication with them for good.
- **Failure:** The C2 servers are misidentified. Data exfiltration continues. Additional infrastructure gets affected (RL + $100,000, RC +$50,000).

If one member fails, another one can roll, on a rotation basis (the member with highest TA has precedence). This has to be rolled till the action succeeds.

Then roll for **Incident Response + Stress Management (DC 12)** to start the recovery process by reactivating basic services. This is a critical juncture in the exercise and only one roll will be possible. It is recommended that the team member with the highest TA takes the roll.

- **Success:** Backup infrastructure and configurations are available. Basic operations and functionalities are restored and back online. Congratulations! The team can now see the light at the end of the tunnel.
- **Failure:** Backup infrastructure and data is unavailable or corrupted! The company does not have a proper recovery plan including additional infrastructure and basic backups. This is a critical failure. Be sure it never happens in real life! (RF+$200,000)

If this skill roll is successful, move to Act 3.

If, on the other hand, the roll failed, the CISO and the management team now have to decide whether to pay the ransom or not.

If the ransom is not paid, then all data is lost. The company gets RL+100,000,000 and RC+10,000,000 as everything needs to be rebuild from scratch.

This choice concludes the TTX.

If the management team decides to pay the ransom, CISO rolls for **Policy Compliance + Stress Management (DC 16)**.

- **Success:** You got lucky! The key received from the cybercriminals actually works. RC+$8,880,000 due to the ransom payment (RF+$200,000).
- **Failure:** The criminal gang disappeared with the money. This is a total disaster. The Company gets RL+100,000,000 and RC+18,880,000 as

everything needs to be rebuild from scratch, plus the ransom (RF+$200,000).

Either way, after this roll, the TTX is over.

Act 3: Recovery and Long-Term Consequences

Congratulations! The team is doing well and is on the path to recovery. Now the following tasks need to be taken care of:

- Decrypting systems or restoring from backups
- Internal security overhaul and investigation to prevent recurrence
- Ongoing compliance reviews and regulatory inquiries

The team has to reference the following:

- Ransomware Playbook
    - Section 5: (Investigation) to learn more about the attackers and their modus operandi
    - Section 6: (Eradication and Recovery) for operational restoration
    - Section 7: (Communication and Reporting) for dealing with customers and stakeholders at all levels
- IRP Section 6 for post-mortem procedures

Skill Checks:

The **FI** and/or the **ISA** can check for specific information about the malware. Maybe some decryption keys were made available online by some research group.

For the **FI**, roll **Forensic Analysis (DC 16)** to analyze ransomware encryption. For the **ISA** roll **Threat Analysis (DC 17)** instead.

- **Success:** A decryption method is found, saving the $8.88 million ransom! Everyone is impressed with this result and PR can make a good story about it. Reputation increases (RD −2).
- **Failure:** Encryption is unbreakable, forcing alternative recovery efforts.

If failure, the next step is to restore from backups.

RM to roll skill check on **Policy Compliance (DC 12)** to evaluate status of data and configurations backups.

- **Success:** Everything is in order. All databases and relevant configurations had regular backups that were safely stored offline (RD−1).
- **Failure:** The latest backups were still in the cloud and were not moved offline yet. They were encrypted by the ransomware, too, forcing the team to restore from a much older version. Hence, overall recovery efforts have increased significantly, together with additional regulatory enquiries (RF+$100,000, RC+$300,000).

NetAdmin to roll skill check on **System Configuration (DC 14)**.

- **Success:** Everything works. Damage has finally been contained! (RD–1)
- **Failure:** The single offline copy of the latest backup fails! The team needs to restore from an older version (RF+$100,000, RC+$300,000).

If either roll failed, the CISO should lead the team to decide whether negotiate and pay the ransom to retrieve the latest version or to accept the current outcome. If successful, this would halve the projected RL and cancel all RC incurred so far, but failure would have serious financial and reputation implications. This leads to a similar skill check and outcome to what we saw in Act 2 after the attempt of restoring the basic infrastructure failed. Either way, this will lead to the end of the exercise.

If the management team decides to pay the ransom, CISO rolls for **Policy Compliance + Stress Management (DC 16)**.

- **Success:** You got lucky! The key received from the cybercriminals actually works. RC+$8,880,000 due to the ransom payment. RL is halved. RC are reset (RF+$200,000).
- **Failure:** The criminal gang disappeared with the money. The Company gets RL+10,000,000 and RC+8,880,000 (RD+5, RF+$500,000).

For this exercise, the overall team performance can be evaluated according to the different damage metrics:

- If RL is less than $500,000, award 1 XP to all team members.
- If RD is less than 3, award 1 XP to all team members.
- If RFs are less than $200,000, award 1 XP to all team members.
- If RCs are less than $200,000, award 1 XP to all team members.

To conclude, the CGM should lead the post incident review. Is there any way this scenario could have actually happened in the company the TTX was run in? If the team is confused, pick a possible topic such as lack of second factor authentication, mismanaged privileges, patching and updating policies, network segmentation to isolate specific servers etc. and verify with the team how it is handled across the company. Could that be a potential weakness?

Comments and Additional Ideas

In such a critical scenario, one of the CGM’s primary responsibilities is escalating consequences based on the possible failure points as the attack unfolds, making the team “feel the pain” for all the possible things that can go wrong. As usual, the CGM should feel free to improvise on the provided script and add additional elements, especially if they are relevant to the context of the organization running the TTX.

For example, to make things more realistic, if the ISA fails to detect the initial breach, the CGM can also inject false forensic leads, forcing the team to waste valuable time and increase some costs accordingly. If the team decides to pay the ransom, which is never recommended, the CGM may have regulators step in early, increasing legal scrutiny and possibly make the team rethink their decisions.

Since there are several damage metrics in this example, the CGM must also track each of them in real-time. Note that financial damages should be adjusted to feel like a realistic outcome to the specific organization that is running the exercise and more can also be added, like possible stock price movements whenever the reputation of the company is affected. A poorly handled PR response could also result in client lawsuits and additional regulatory penalties, too. If any compliance aspect is neglected or handled poorly, the CGM can decide to escalate this and introduce government intervention, increasing long-term financial consequences.

Adding additional unexpected injects always adds replayability to the scenario and keeps players engaged. In this context, if the team successfully mitigates the ransomware encryption, the CGM could introduce a secondary extortion attempt where attackers claim to have a deeper foothold and demand another payment. Are they bluffing? Who knows? If the team does not thoroughly investigate, though, they may wrongly assume the attack is over, setting the stage for a repeat breach scenario, which can even be expanded in a follow-up exercise. Remember: in RPGs, a quest is usually part of a bigger campaign that can potentially last a very, very long time. Here we can also adopt a similar approach where team members may have to continue defending their organization across multiple sessions as a possible threat may unfold in something unexpected or have a follow-up attack.

It is also important to keep stressing how the CGM needs to monitor how well the team follows the official documentation. If they skip on any relevant section of the IRP or ransomware playbook, we can introduce delays due to some confusion and misunderstandings between departments and make some action fail with dramatic consequences. Conversely, we can

also reward initiative and correct execution with additional XP bonuses or reduced penalties, so as to incentivize methodical decision-making.

Inter-team communication and role execution should also be another area of focus for the CGM. Here, we need to keep the proper balance and the team needs to work, well, as a real team! If the CISO wants to dominate all decision-making without input from technical roles whenever appropriate, the CGM may introduce a technical oversight and do a skill check based on the CISO's technical stats, possibly leading to serious consequences and setbacks.

Last but not least, we should remember that the time an actual team can dedicate to these exercises has to be limited and each session should be timeboxed to 1–2 hours only, regardless of how fun and engaging all this is. If the team is struggling excessively, we can allow an external security consultant to provide hints and possible intervention, reflecting real-world vendor support. However, this "Deus ex machina" approach should be a last resort and the team will need to address their lack of understanding of the problem in a separate session. On the other hand, if the team resolves all the challenges too quickly, we may decide to introduce new technical hurdles, such as confidential files leaking on the dark web or a more dangerous strain of malware that was hiding in the server BIOS/UEFI firmware and survived a hard disk backup.

Like in an RPG, the original scenario is always just a canvas upon which new, unexpected adventures can unfold to fit the players' skills and satisfy their thirst for the unknown.

Notes

1. https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/ ⏎
2. https://attack.mitre.org/techniques/T1078/003/ ⏎
3. https://attack.mitre.org/techniques/T1078/004/ ⏎
4. https://attack.mitre.org/techniques/T1133/ ⏎
5. https://attack.mitre.org/techniques/T1486/ ⏎

6. https://attack.mitre.org/techniques/T1567/002/ ⏎
7. https://attack.mitre.org/techniques/T1571/001/ ⏎

Appendix A

Note: This template is just a high-level starting point that has to be tailored to the specific needs and characteristics of a given company by considering its specific size, industry, and regulatory requirements.

Incident Response Plan Template

Version 1.0 | [Date]

1. Introduction

1.1 Purpose of the Plan

The IRP outlines the procedures and protocols to be followed in the event of a cybersecurity incident within [Company Name]. The primary goal is to mitigate the impact of incidents, maintain business continuity, and safeguard sensitive information.

1.2 Scope

This plan encompasses all employees, systems, and data within [Company Name]. It applies to cybersecurity incidents that could compromise the confidentiality, integrity, or availability of information assets.

1.3 Objectives

- Rapid identification and containment of security incidents
- Efficient coordination among response teams

- Preservation of evidence for forensic analysis
- Prevention of future incidents through lessons learned

2. Roles and Responsibilities: Incident Response Team (IRT)

2.1 The Incident Response Team (IRT)

Identify and designate key members of the IRT, including their roles and responsibilities. This may include representatives from IT, legal, communications, and management.

2.2 Contact Information

Maintain up-to-date contact information for all members of the IRT. Ensure that this information is easily accessible and known to relevant personnel.

3. Incident Classification

3.1 Incident Severity Levels and Categories

Define and categorize potential incidents based on severity and impact. Classify incidents into categories such as low, medium, high, and critical.

3.2 Types of Incidents

Include anything relevant, for example, Ransomware, DDoS, etc.

3.2 Incident Reporting

Establish clear reporting procedures for employees to report potential incidents promptly. Include contact information for the IRT and the preferred reporting channels.

4. Incident Response Lifecycle

4.1 Detection Mechanisms

Outline methods for detecting potential incidents, such as IDS, log analysis, and employee reporting.

4.2 Initial Assessment

Detail the steps for conducting an initial assessment of the incident, including the gathering of relevant information and the determination of severity.

5. Incident Containment and Eradication

5.1 Containment

Define procedures for isolating and containing the incident to prevent further damage.

5.2 Eradication

Provide guidelines for the removal of the incident, including the elimination of malware, unauthorized access, or other compromising factors.

6. Communication and Notification

6.1 Internal Communication

Establish communication protocols within the organization to ensure that all relevant stakeholders are informed appropriately.

6.2 External Communication

Define procedures for communicating with external parties, including regulatory bodies, customers, and law enforcement if necessary.

7. Recovery and Lessons Learned

7.1 Restoration of Systems

Outline the steps for restoring affected systems and services to normal operation.

7.2 Post-Incident Review

Conduct a post-incident review to analyze the response, identify areas for improvement, and update the IRP accordingly.

8. Training and Awareness

8.1 Employee Training

Provide ongoing training and awareness programs for employees to recognize and respond effectively to potential cybersecurity incidents.

8.2 Plan Review and Testing

Regularly review and test the IRP to ensure its effectiveness and relevance.

9. Plan Maintenance

9.1 Document Versioning

Maintain version control for the IRP and update it as necessary based on changes in technology, personnel, or organizational structure.

10. Contact Information

Provide updated contact information for key stakeholders and members of the IRT.

Appendix B

Note: This template is just a starting point that needs to be customized based on a specific incident, organization’s unique needs, response team structure, and specific technologies in use.

Incident Playbook Template

Version 1.0 | [Date]
Incident Type: [Specify Incident Type]

1. Incident Overview

1.1 Description

Provide a brief description of the incident type, including common indicators, symptoms, or triggers.

1.2 Objective

Clearly state the goals and objectives for responding to this specific incident.

2. Initial Detection and Assessment

2.1 Detection

Describe how this type of incident is typically detected. Include information on monitoring tools, alerts, or user reports.

2.2 Assessment

Outline the initial steps for assessing the severity and scope of the incident.

3. Incident Response Team Activation

3.1 Team Roles

Specify the roles and responsibilities of each team member involved in responding to this incident.

3.2 Communication Plan

Provide a communication plan, including contact information for key team members and external stakeholders.

4. Containment and Mitigation

4.1 Isolation

Detail the steps for isolating affected systems or networks to prevent further damage.

4.2 Mitigation

Outline specific actions to mitigate the impact of the incident and prevent its spread.

5. Investigation and Analysis

5.1 Forensic Analysis

Define procedures for conducting forensic analysis to determine the root cause and extent of the incident.

5.2 Data Collection

Specify the information to be collected during the investigation, such as logs, artifacts, or network traffic.

6. Eradication and Recovery

6.1 Eradication

Provide steps for removing the incident and associated threats from the environment.

6.2 System Recovery

Outline the procedures for restoring affected systems to normal operation.

7. Communication and Reporting

7.1 Internal Communication

Detail the internal communication plan, including updates to staff and management.

7.2 External Communication

Specify procedures for communicating with external parties, such as customers, regulatory bodies, or law enforcement.

8. Lessons Learned and Documentation

8.1 Post-Incident Review

Describe the process for conducting a post-incident review to identify improvements and lessons learned.

8.2 Documentation

Emphasize the importance of thorough documentation for regulatory compliance and continuous improvement.

Appendix C

RPG-TTX Character Sheet

Name: _____
Role: _____ (e.g., Red Teamer)
Level: _____ XP: _____ / _____

XP System: XP is awarded for passing challenges according to the formula: DC/10, rounded to the nearest integer. Level Progression: XP required to level up = 10 × Current Level

Table C.1 Primary stats (Base: 4D6, drop lowest, max 18, min 3 before bonuses)

STAT	ABBREVIATION	VALUE	MOD (FLOOR((VALUE-10)/2))
Technical Acumen	TA		
Strategic Thinking	ST		
Analytical Skills	AN		
Resilience	RES		
Communication	COM		
Leadership	LDR		

Modifiers: For every 2 points above 10, add +1 to relevant skills. For every 2 points below 10, subtract 1.

Table C.2 Derived skills (Base = Sum of relevant stat modifiers + role bonuses + Level)

SKILL	RELEVANT STATS BONUSES	ROLE BONUS	LEVEL TOTAL
Threat Analysis	AN + TA		
Incident Response	TA + RES		
Forensic Analysis	TA + AN		
System Configuration	TA + ST		
Policy Compliance	ST + COM		
Risk Assessment	ST + AN		
Stakeholder Engagement	COM + LDR		
Stress Management	RES + COM		

Optional Fields (To Be Customized by the CGM as Needed)

Inventory & Resources

Tools & Equipment:

- _____
- _____
- _____

Access Privileges:

- _____

Network Permissions:

- _____

Abilities & Perks (from Role or Level Progression)

1. _____
2. _____
3. _____

Appendix D

Pre-Rolled Characters

This appendix provides a set of pre-rolled (i.e., ready-made) characters, one for each specific role, ready to use in case the team does not wish to create new ones. Every character is designed to be good at their specific tasks from the get-go, that is, from Level 1 already, so they are a good choice for beginners.

Specifically:

- Philip Firewall, an ISA who is always ready to spot anything unexpected
- Rudy Router, a calm and collected NetAdmin who won't lose track of things
- Barry Breacher, an RT constantly looking for weak points and vulnerabilities to exploit
- Trudy Tracer, an FI who follows digital trails like a bloodhound
- Steve Server, a Chief Technology Information Officer and an old-school guy who is reliable and gets the job done, no matter what
- Margaret Margin, an experienced RM who calculates everything with extreme precision
- Patty Policy, a reliable HR Manager. She loves employee handbooks and knows how to resolve conflicts
- Clarence Clause, a LA who is a stickler for legal details and contracts
- Holly Headline, a PR Specialist/Manager who knows how to craft the perfect media statement

Philip Firewall – ISA

Name: Philip Firewall Role: ISA
Level: _____ XP: _____ / _____

XP System: XP is awarded for passing challenges according to the formula: DC/10, rounded to the nearest integer. Level Progression: XP required to level up = 10 × Current Level

Stats Philip Firewall Primary stats (Base: 4D6, drop lowest, max 18, min 3 before bonuses)

STAT	ABBREVIATION	VALUE	MOD (FLOOR((VALUE-10)/2))
Technical Acumen	TA	15	2
Strategic Thinking	ST	13	1
Analytical Thinking	AN	14	2
Resilience	RES	12	1
Communication	COM	10	0
Leadership	LDR	8	-1

Modifiers: For every 2 point above 10, add +1 to relevant skills. For every 2 points below 10, subtract 1.

Skills Philip Firewall Derived skills (Base = Sum of relevant stat modifiers + role bonuses + Level)

SKILL	RELEVANT STATS BONUSES	ROLE BONUS	LEVEL	TOTAL
Threat Analysis	AN + TA: 4	1	1	6
Incident Response	TA + RES: 3	1	1	5
Forensic Analysis	TA + AN: 4	1	1	6

SKILL	RELEVANT STATS BONUSES	ROLE BONUS	LEVEL	TOTAL
System Configuration	TA + ST: 3	1	1	5
Policy Compliance	ST + COM: 1		1	2
Risk Assessment	ST + AN: 3		1	4
Stakeholder Engagement	COM + LDR: -1		1	0
Stress Management	RES + COM: 1		1	2

Rudy Router – Network Administrator
Name: Rudy Router Role: Network Admin
Level: _____ XP: _____ / _____

XP System: XP is awarded for passing challenges according to the formula: DC/10, rounded to the nearest integer. Level Progression: XP required to level up = 10 × Current Level

Stats Rudy Router Primary stats (Base: 4D6, drop lowest, max 18, min 3 before bonuses)

STAT	ABBREVIATION	VALUE	MOD (FLOOR((VALUE-10)/2))
Technical Acumen	TA	14	2
Strategic Thinking	ST	10	0
Analytical Thinking	AN	12	1
Resilience	RES	13	1
Communication	COM	6	-2
Leadership	LDR	8	-1

Modifiers: For every 2 point above 10, add +1 to relevant skills. For every 2 points below 10, subtract 1.

Skills Rudy Router Derived skills (Base = Sum of relevant stat modifiers + role bonuses + Level)

SKILL	RELEVANT STATS BONUSES	ROLE BONUS	LEVEL	TOTAL
Threat Analysis	AN + TA: 3	1	1	5
Incident Response	TA + RES: 3	1	1	5
Forensic Analysis	TA + AN: 3		1	4
System Configuration	TA + ST: 2	2	1	5
Policy Compliance	ST + COM: -2		1	-1
Risk Assessment	ST + AN: 1		1	2
Stakeholder Engagement	COM + LDR: -3		1	-2
Stress Management	RES + COM: -1		1	0

Barry Breacher – Red Teamer
Name: Barry Breacher Role: Red Teamer/White Hat Hacker
Level: _____ XP: _____ / _____

XP System: XP is awarded for passing challenges according to the formula: DC/10, rounded to the nearest integer. Level Progression: XP required to level up = 10 × Current Level

Stats Barry Breacher Primary stats (Base: 4D6, drop lowest, max 18, min 3 before bonuses)

STAT	ABBREVIATION	VALUE	MOD (FLOOR((VALUE-10)/2))
Technical Acumen	TA	13	1

STAT	ABBREVIATION	VALUE	MOD (FLOOR((VALUE-10)/2))
Strategic Thinking	ST	11	0
Analytical Thinking	AN	15	2
Resilience	RES	13	1
Communication	COM	10	0
Leadership	LDR	8	-1

Modifiers: For every 2 point above 10, add +1 to relevant skills. For every 2 points below 10, subtract 1.

Skills Barry Breacher Derived skills (Base = Sum of relevant stat modifiers + role bonuses + Level)

SKILL	RELEVANT STATS BONUSES	ROLE BONUS	LEVEL	TOTAL
Threat Analysis	AN + TA: 3	2	1	6
Incident Response	TA + RES: 2	2	1	5
Forensic Analysis	TA + AN: 3		1	4
System Configuration	TA + ST: 1	1	1	3
Policy Compliance	ST + COM: 0		1	1
Risk Assessment	ST + AN: 2		1	3
Stakeholder Engagement	COM + LDR: -1		1	0
Stress Management	RES + COM: 1		1	2

Trudy Tracer – Forensic Investigator

Name: Trudy Tracer Role: Forensic Investigator

Level: _____ XP: _____ / _____

XP System: XP is awarded for passing challenges according to the formula: DC/10, rounded to the nearest integer. Level Progression: XP required to level up = 10 × Current Level

Stats Trudy Tracer Primary stats (Base: 4D6, drop lowest, max 18, min 3 before bonuses)

STAT	ABBREVIATION	VALUE	MOD (FLOOR((VALUE-10)/2))
Technical Acumen	TA	12	1
Strategic Thinking	ST	10	0
Analytical Thinking	AN	14	2
Resilience	RES	16	3
Communication	COM	11	0
Leadership	LDR	10	0

Modifiers: For every 2 point above 10, add +1 to relevant skills. For every 2 points below 10, subtract 1.

Skills Trudy Tracer Derived skills (Base = Sum of relevant stat modifiers + role bonuses + Level)

SKILL	RELEVANT STATS BONUSES	ROLE BONUS	LEVEL	TOTAL
Threat Analysis	AN + TA: 3	1	1	5
Incident Response	TA + RES: 4		1	5
Forensic Analysis	TA + AN: 3	2	1	6
System Configuration	TA + ST: 1	1	1	3
Policy Compliance	ST + COM: 0		1	1
Risk Assessment	ST + AN: 2		1	3

SKILL	RELEVANT STATS BONUSES	ROLE BONUS	LEVEL	TOTAL
Stakeholder Engagement	COM + LDR: 0		1	1
Stress Management	RES + COM: 3		1	4

Steve Server – Chief Technology Information Officer
Name: Steve Server Role: CISO
Level: _____ XP: _____ / _____

XP System: XP is awarded for passing challenges according to the formula: DC/10, rounded to the nearest integer. Level Progression: XP required to level up = 10 × Current Level

Stats Steve Server Primary stats (Base: 4D6, drop lowest, max 18, min 3 before bonuses)

STAT	ABBREVIATION	VALUE	MOD (FLOOR((VALUE-10)/2))
Technical Acumen	TA	12	1
Strategic Thinking	ST	13	1
Analytical Thinking	AN	15	2
Resilience	RES	10	0
Communication	COM	12	1
Leadership	LDR	14	2

Modifiers: For every 2 point above 10, add +1 to relevant skills. For every 2 points below 10, subtract 1.

Skills Steve Server Derived skills (Base = Sum of relevant stat modifiers + role bonuses + Level)

SKILL	RELEVANT STATS BONUSES	ROLE BONUS	LEVEL	TOTAL
Threat Analysis	AN + TA: 3		1	4
Incident Response	TA + RES: 1		1	2
Forensic Analysis	TA + AN: 3		1	4
System Configuration	TA + ST: 2		1	3
Policy Compliance	ST + COM: 2	1	1	4
Risk Assessment	ST + AN: 3	1	1	5
Stakeholder Engagement	COM + LDR: 3	2	1	6
Stress Management	RES + COM: 1	1	1	3

Margaret Margin – Risk Manager
Name: Margaret Margin Role: Risk Manager
Level: _____ XP: _____ / _____

XP System: XP is awarded for passing challenges according to the formula: DC/10, rounded to the nearest integer. Level Progression: XP required to level up = 10 × Current Level

Stats Margaret Margin Primary stats (Base: 4D6, drop lowest, max 18, min 3 before bonuses)

STAT	ABBREVIATION	VALUE	MOD (FLOOR((VALUE-10)/2))
Technical Acumen	TA	10	0
Strategic Thinking	ST	12	1
Analytical Thinking	AN	11	0
Resilience	RES	13	1

STAT	ABBREVIATION	VALUE	MOD (FLOOR((VALUE-10)/2))
Communication	COM	14	2
Leadership	LDR	15	2

Modifiers: For every 2 point above 10, add +1 to relevant skills. For every 2 points below 10, subtract 1.

Skills Margaret Margin Derived skills (Base = Sum of relevant stat modifiers + role bonuses + Level)

SKILL	RELEVANT STATS BONUSES	ROLE BONUS	LEVEL	TOTAL
Threat Analysis	AN + TA: 0		1	1
Incident Response	TA + RES: 1		1	2
Forensic Analysis	TA + AN: 0		1	1
System Configuration	TA + ST: 1		1	2
Policy Compliance	ST + COM: 3	2	1	6
Risk Assessment	ST + AN: 1	2	1	4
Stakeholder Engagement	COM + LDR: 4	1	1	6
Stress Management	RES + COM: 3		1	4

Patty Policy – Human Resource Manager
Name: Patty Policy Role: HR Manager
Level: _____ XP: _____ / _____

XP System: XP is awarded for passing challenges according to the formula: DC/10, rounded to the nearest integer. Level Progression: XP required to level up = 10 × Current Level

Stats Patty Policy Primary stats (Base: 4D6, drop lowest, max 18, min 3 before bonuses)

STAT	ABBREVIATION	VALUE	MOD (FLOOR((VALUE-10)/2))
Technical Acumen	TA	6	-2
Strategic Thinking	ST	10	0
Analytical Thinking	AN	11	0
Resilience	RES	15	2
Communication	COM	16	3
Leadership	LDR	14	2

Modifiers: For every 2 point above 10, add +1 to relevant skills. For every 2 points below 10, subtract 1.

Skills Patty Policy Derived skills (Base = Sum of relevant stat modifiers + role bonuses + Level)

SKILL	RELEVANT STATS BONUSES	ROLE BONUS	LEVEL	TOTAL
Threat Analysis	AN + TA: -2		1	-1
Incident Response	TA + RES: 0		1	1
Forensic Analysis	TA + AN: -2		1	-1
System Configuration	TA + ST: -2		1	-1
Policy Compliance	ST + COM: 3	1	1	5
Risk Assessment	ST + AN: 0		1	1
Stakeholder Engagement	COM + LDR: 5	1	1	7
Stress Management	RES + COM: 5	2	1	8

Clarence Clause – Legal Advisor
Name: Clarence Clause Role: Legal Advisor
Level: _____ XP: _____ / _____

XP System: XP is awarded for passing challenges according to the formula: DC/10, rounded to the nearest integer. Level Progression: XP required to level up = 10 × Current Level

Stats Clarence Clause Primary stats (Base: 4D6, drop lowest, max 18, min 3 before bonuses)

STAT	ABBREVIATION	VALUE	MOD (FLOOR((VALUE-10)/2))
Technical Acumen	TA	6	-2
Strategic Thinking	ST	12	1
Analytical Thinking	AN	11	0
Resilience	RES	10	0
Communication	COM	14	2
Leadership	LDR	13	1

Modifiers: For every 2 point above 10, add +1 to relevant skills. For every 2 points below 10, subtract 1.

Skills Clarence Clause Derived skills (Base = Sum of relevant stat modifiers + role bonuses + Level)

SKILL	RELEVANT STATS BONUSES	ROLE BONUS	LEVEL	TOTAL
Threat Analysis	AN + TA: -2		1	-1
Incident Response	TA + RES: -2		1	-1
Forensic Analysis	TA + AN: -2		1	-1

SKILL	RELEVANT STATS BONUSES	ROLE BONUS	LEVEL	TOTAL
System Configuration	TA + ST: -1		1	0
Policy Compliance	ST + COM: 3	2	1	6
Risk Assessment	ST + AN: 1		1	2
Stakeholder Engagement	COM + LDR: 3	1	1	5
Stress Management	RES + COM: 2	1	1	4

Holly Headline – Public Relation Specialist/Manager
Name: Holly Headline Role: PR Manager
Level: _____ XP: _____ / _____

XP System: XP is awarded for passing challenges according to the formula: DC/10, rounded to the nearest integer. Level Progression: XP required to level up = 10 × Current Level

Stats Holly Headline Primary stats (Base: 4D6, drop lowest, max 18, min 3 before bonuses)

STAT	ABBREVIATION	VALUE	MOD (FLOOR((VALUE-10)/2))
Technical Acumen	TA	8	-1
Strategic Thinking	ST	12	1
Analytical Thinking	AN	13	1
Resilience	RES	10	0
Communication	COM	15	2
Leadership	LDR	16	3

Index